Exhibit D

US011620634B2

(12) **United States Patent**
Wyatt

(10) **Patent No.: US 11,620,634 B2**
(45) **Date of Patent: *Apr. 4, 2023**

(54) **MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE**

(71) Applicant: **CARDWARE, INC**, San Jose, CA (US)

(72) Inventor: **David Wyatt**, Austin, TX (US)

(73) Assignee: **CARDWARE, INC.**, Austin, TX (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **17/528,073**

(22) Filed: **Nov. 16, 2021**

(65) **Prior Publication Data**

US 2022/0207517 A1 Jun. 30, 2022

Related U.S. Application Data

(60) Continuation of application No. 17/075,637, filed on Oct. 20, 2020, now Pat. No. 11,176,538, which is a (Continued)

(51) **Int. Cl.**
G06Q 20/34 (2012.01)
G07F 19/00 (2006.01)
(Continued)

(52) **U.S. Cl.**
CPC ***G06Q 20/341*** (2013.01); ***G06K 19/06206*** (2013.01); ***G06K 19/0716*** (2013.01);
(Continued)

(58) **Field of Classification Search**
CPC G06Q 20/341; G06Q 20/06; G06Q 20/065; G06Q 20/223; G06Q 20/24;
(Continued)

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,736,322 B2 5/2004 Gobburu et al.
7,100,821 B2 9/2006 Rasti
(Continued)

FOREIGN PATENT DOCUMENTS

GB	2478712	9/2011
GB	2485442	5/2012
WO	00/62214	10/2000
WO	01/57620	8/2001
WO	2005119607	12/2005
WO	2007145687	12/2007

(Continued)

OTHER PUBLICATIONS

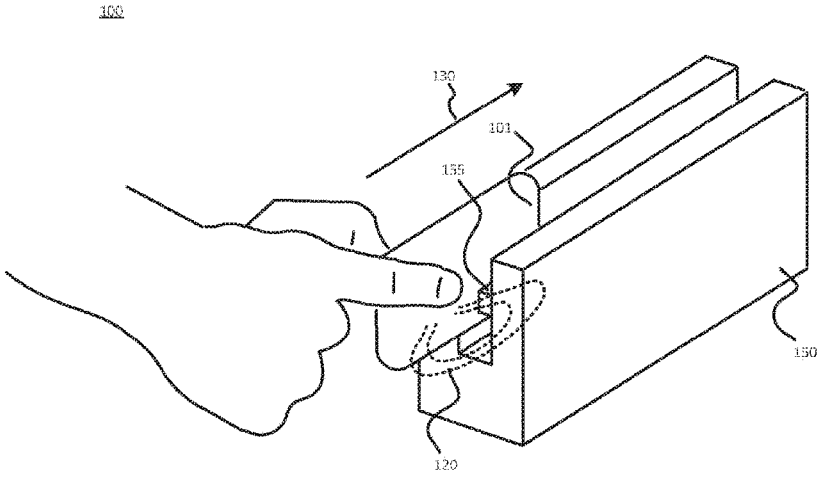
"Isis NFC-payment from SXSW 2012," YouTube, https://www.youtube.com/watch?v=Z2MOAtUhR7k, Mar. 10, 2012, pp. 1-2.
(Continued)

Primary Examiner — Seung H Lee

(57) **ABSTRACT**

An embodiment includes a multi-function electronic device capable of generating a programmed magnetic field of alternating polarity based on a speed of a card swipe, and methods for constructing the device for the purpose of emulating a standard credit card. An apparatus is described to allow the device to emulate behavior of a credit card when used in electronic credit card readers. Additionally, methods are described to allow user control of the device for the purpose of authorizing or controlling use of the device in the application of credit, debit and cash transactions, including cryptocurrency and device-to-device transactions. Methods are also described for generating a limited-duration payment number when performing a transaction for the purpose of creating a limited-use payment number, which is limited in scope of use to a predetermined number of authorized transactions. Furthermore the device may interact with other similar devices in proximity for the purpose of funds or credit/debit transfers.

72 Claims, 7 Drawing Sheets



Related U.S. Application Data

continuation of application No. 16/459,150, filed on Jul. 1, 2019, now Pat. No. 10,810,579, which is a continuation of application No. 15/701,261, filed on Sep. 11, 2017, now Pat. No. 10,339,520, which is a continuation of application No. 14/981,757, filed on Dec. 28, 2015, now Pat. No. 9,760,884, which is a continuation of application No. 14/680,979, filed on Apr. 7, 2015, now Pat. No. 9,224,083, which is a division of application No. 14/217,261, filed on Mar. 17, 2014, now Pat. No. 9,022,286.

(60) Provisional application No. 61/794,891, filed on Mar. 15, 2013.

(51) **Int. Cl.**

G06Q 20/06	(2012.01)
G06Q 20/22	(2012.01)
G06Q 20/38	(2012.01)
G07F 7/08	(2006.01)
G06K 19/06	(2006.01)
G06K 19/07	(2006.01)
G06K 19/077	(2006.01)
G06Q 20/24	(2012.01)
G06Q 20/40	(2012.01)

(52) **U.S. Cl.**

CPC ***G06K 19/07749*** (2013.01); ***G06Q 20/06*** (2013.01); ***G06Q 20/065*** (2013.01); ***G06Q 20/223*** (2013.01); ***G06Q 20/24*** (2013.01); ***G06Q 20/346*** (2013.01); ***G06Q 20/347*** (2013.01); ***G06Q 20/352*** (2013.01); ***G06Q 20/385*** (2013.01); ***G06Q 20/3827*** (2013.01); ***G06Q 20/409*** (2013.01); ***G06Q 20/4012*** (2013.01); ***G07F 7/0873*** (2013.01); ***G07F 19/00*** (2013.01)

(58) **Field of Classification Search**

CPC .. G06Q 20/346; G06Q 20/347; G06Q 20/352; G06Q 20/3827; G06Q 20/385; G06Q 20/4012; G06Q 20/409; G06K 19/06206; G06K 19/0716; G06K 19/07749; G07F 7/0873; G07F 19/00

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

7,690,580	B2	4/2010	Shoemaker
7,967,211	B2	6/2011	Challa et al.
8,255,323	B1	8/2012	Casey et al.
8,423,462	B1	4/2013	Amacker et al.
8,499,334	B2	7/2013	Doughty et al.
8,571,937	B2	10/2013	Rose et al.
8,628,012	B1	1/2014	Wallner
8,690,055	B2	4/2014	Anderson et al.
8,690,059	B1	4/2014	Wallner
8,814,046	B1	8/2014	Wallner
9,098,846	B2	8/2015	Gill et al.
9,105,020	B2	8/2015	Ronca et al.
9,361,613	B2	6/2016	Wallner
9,454,679	B2	9/2016	Wallner
9,600,808	B1	3/2017	Gomez, Sr. et al.
9,652,642	B2	5/2017	Wallner
9,818,104	B1	11/2017	Katzer et al.
9,846,866	B2	12/2017	Royyuru
9,864,994	B2	1/2018	Huang et al.
10,037,524	B2	7/2018	Royyuru et al.
10,044,510	B2	8/2018	Kwon et al.
10,269,005	B2	4/2019	Lee et al.
10,275,761	B2	4/2019	Lee et al.
10,402,811	B2	9/2019	Park et al.
10,423,942	B2	9/2019	Lee et al.
10,454,728	B2	10/2019	Huang
10,460,314	B2	10/2019	Hird et al.
10,505,277	B2	12/2019	Lee et al.
10,516,208	B2	12/2019	Lee et al.
10,540,647	B2	1/2020	Park et al.
10,546,291	B2	1/2020	Kim et al.
10,592,893	B2	3/2020	Lee et al.
10,680,322	B2	6/2020	Lee et al.
10,699,266	B2	6/2020	Lee et al.
10,713,646	B1	7/2020	Lee et al.
10,796,299	B2	10/2020	Lee et al.
10,803,452	B2	10/2020	Kim et al.
10,862,718	B2	12/2020	Huang
10,902,390	B2	1/2021	Lee et al.
10,929,851	B2	2/2021	Kang et al.
10,990,954	B2	4/2021	Park et al.
10,990,959	B2	4/2021	Lee et al.
10,998,620	B2	5/2021	Lee et al.
11,004,075	B2	5/2021	Lee et al.
11,017,399	B2	5/2021	Park et al.
11,042,855	B2	6/2021	Kim et al.
11,061,698	B2	7/2021	Rhee et al.
11,074,581	B2	7/2021	Kim et al.
11,100,431	B2	8/2021	Mullen et al.
11,107,047	B2	8/2021	Kim et al.
11,127,010	B2	9/2021	Cho et al.
11,129,018	B2	9/2021	Kim et al.
11,227,278	B2	1/2022	Choi et al.
11,232,339	B2	1/2022	Lee et al.
11,321,701	B2	5/2022	Lee et al.
2002/0153424	A1	10/2002	Li
2005/0043997	A1	2/2005	Sahota et al.
2006/0089171	A1	4/2006	Yoo et al.
2008/0126260	A1	5/2008	Cox et al.
2008/0172317	A1	7/2008	Deibert et al.
2008/0222047	A1	9/2008	Boalt
2008/0302876	A1	12/2008	Mullen
2008/0319905	A1	12/2008	Carlson
2009/0048971	A1	2/2009	Hathaway et al.
2009/0159701	A1	6/2009	Mullen et al.
2010/0185545	A1	7/2010	Royyuru et al.
2011/0186626	A1	8/2011	Manessis et al.
2011/0276416	A1	11/2011	Mullen et al.
2012/0310760	A1	12/2012	Phillips et al.
2012/0317035	A1	12/2012	Royyuru et al.
2013/0124410	A1	5/2013	Kay et al.
2013/0166441	A1	6/2013	Kobylkin et al.
2013/0232083	A1	9/2013	Smith et al.
2013/0262305	A1	10/2013	Jones et al.
2014/0143785	A1	5/2014	Mistry et al.
2015/0147065	A1	5/2015	Civelli et al.
2015/0178724	A1	6/2015	Ngo et al.
2015/0317632	A1	11/2015	Park et al.
2016/0132881	A1	5/2016	Lee et al.
2016/0253652	A1	9/2016	Je et al.
2016/0253657	A1	9/2016	Sohn et al.
2019/0026725	A1	1/2019	Park et al.
2019/0172051	A1	6/2019	Lee et al.
2019/0173290	A1	6/2019	Ha et al.
2021/0311752	A1	10/2021	Rhee et al.
2022/0005046	A1	1/2022	Kim et al.

FOREIGN PATENT DOCUMENTS

WO	2010043974	4/2010
WO	2012154915	11/2012
WO	2012154915 A1	11/2012

OTHER PUBLICATIONS

"Isis NFC-payment from SXSW 2012," Transcript of YouTube, https://www.youtube.com/watch?v=Z2MOAtUhR7k, Mar. 10, 2012, pp. 1-3.

"NFC—Google Wallet and More—EE Times—Mobile World Congress," YouTube, https://www.youtube.com/watch?v=AgSk7L6HhVw, Mar. 6, 2012, pp. 1-3.

(56) **References Cited**

OTHER PUBLICATIONS

"NFC—Google Wallet and More—EE Times—Mobile World Congress," Transcript of YouTube, https://www.youtube.com/watch?v=AgSk7L6HhVw, Mar. 6, 2012, pp. 1-8.
"Paying With Google Wallet," YouTube, https://www.youtube.com/watch?v=jTeilSlzBPQ, Feb. 6, 2012, pp. 1-2.
"Seinfeld—Google Wallet," YouTube, https://www.youtube.com/watch?v=baaCvgTRYsU, Jun. 14, 2013, pp. 1-2.
"Technology: Google Wallet—The New York Times," YouTube, https://www.youtube.com/watch?v=I8JOT6ban7o, Sep. 23, 2011, pp. 1-2.
"Using Google Wallet in McDonald's!," YouTube, https://www.youtube.com/watch?v= 1p6co4YIvbA, Sep. 14, 2012, pp. 1-2.
"Virtual terminal—#1 storing credit card data with tokenization," YouTube, https://www.youtube.com/watch?v=eSXIIGbACew, Feb. 28, 2011, pp. 1-3.
"What is Google Wallet?," YouTube, https://www.youtube.com/watch?v=iuvyN4iZiP8, Aug. 9, 2011, pp. 1-3.
"What is Tokenization?," YouTube, https://www.youtube.com/watch?v=ypm5FFfEN34, Jan. 17, 2011, pp. 1-3.
"How Credit Card Number Tokenization can Reduce PCI Compliance Stress—File 1 of 3," YouTube, https://www.youtube.com/watch?v=FHD5XzAIKDI, Jul. 28, 2009, pp. 1-3.
"How Credit Card Number Tokenization can Reduce PCI Compliance Stress—File 1 of 3," Transcript of YouTube, https://www.youtube.com/watch?v=FHD5XzAIKDI, Jul. 28, 2009, pp. 1-12.
"How Credit Card Number "Tokenization" Can Reduce PCI Compliance Stress—File 2 of 3," YouTube, https://www.youtube.com/watch?v=t-fWpcLdb3o, Jul. 28, 2009, pp. 1-3.
"How Credit Card Number "Tokenization" Can Reduce PCI Compliance Stress—File 2 of 3," Transcript of YouTube, https://www.youtube.com/watch?v=t-fWpcLdb3o, Jul. 28, 2009, pp. 1-12.
"How Credit Card Number "Tokenization" Can Reduce PCI Compliance Stress—File 3 of 3," YouTube, https://www.youtube.com/watch?v=_CdoKEuEB9s, Jul. 28, 2009, pp. 1-3.
"How Credit Card Number "Tokenization" Can Reduce PCI Compliance Stress—File 3 of 3," Transcript of YouTube, https://www.youtube.com/watch?v=_CdoKEuEB9s, Jul. 28, 2009, pp. 1-8.
"Caixer contactless lacaixa," YouTube, https://www.youtube.com/watch?v=It2CpMcxQC4, Apr. 4, 2011, pp. 1-2.
"Understanding Proximity Sensors—T-Mobile," YouTube, https://www.youtube.com/watch?v=npD48agt0xY, Jan. 2010, pp. 1-2.
"Understanding Proximity Sensors—T-Mobile," YouTube, https://www.youtube.com/watch?v=npD48agt0xY, Jan. 2010, p. 1.
"Understanding Proximity Sensors—T-Mobile," Transcript of YouTube, https://www.youtube.com/watch?v=npD48agt0xY, Jan. 2010, pp. 1-2.
"Google I/O 2012—The Sensitive Side of Android," YouTube, https://www.youtube.com/watch?v=Q0V_Id7iNw4, Jun. 29, 2012, pp. 1-2.
"Google Wallet Overview," YouTube, https://www.youtube.com/watch?v=VuFVsaFCzsw, Aug. 1, 2012, p. 1.
"Google Wallet Overview," Transcript of YouTube, https://www.youtube.com/watch?v=VuFVsaFCzsw, Aug. 1, 2012, pp. 1-2.
"Android 4.0 APIs | Android Developers," mit.edu, https://stuff.mit.edu/afs/sipb/project/android/docs/about/versions/android-4.0.html, 2011, pp. 1-23.
"EMV Integrated Circuit Card Specifications for Payment Systems, Book 2, Security and Key Management, Version 4.3," EMVCo, Nov. 2011, pp. 1-174.
"Exploring Google Wallet using the secure element interface," nelenkov.blogspot.com, Aug. 27, 2012, pp. 1-20.
Garside, "Google Wallet mobile payments system launched to public," The Guardian, https://www.theguardian.com/technology/2011/sep/19/google-wallet-available-public, Sep. 19, 2011, pp. 1-5.
Purdy, "How to grab a screenshot from iPhone, Android, and nearly any other smartphone," Computer World, Apr. 20, 2012, pp. 1-6.
"Maximum failed passcode attempts in restrictions—what happens?," Apple Community, https://discussions.apple.com/thread/3690633, Jan. 2012, pp. 1-3.
"Simplify, Organize & Pay with Loop by Will Graylin & George Wallner," Kickstarter, Mar. 2019, pp. 1-13.
"Hands-on with ISIS Mobile Wallet," YouTube, https://www.youtube.com/watch?v=eOMqvGVKjmM, Mar. 10, 2012, p. 1.
"EMV Solutions," Paragon Application Systems, https://web.archive.org/web/20120818221214/http://www.paragonedge.com/solutions/emv-solutions.html, Aug. 18, 2012, p. 1.
Sullivan, "The Changing Nature of U.S. Card Payment Fraud: Industry and Public Policy Options," Economic Review, Federal Reserve Bank of Kansas City, Second Quarter 2010, ProQuest Information and Learning, vol. 95, No. 2, pp. 101-133.
"EMV Integrated Circuit Card Specifications for Payment Systems, Book 1, Application Independent ICC to Terminal Interface Requirements, Version 4.3," EMVCo, Nov. 2011, pp. 1-189.
"EMV Contactless Specifications for Payment Systems, Book B, Entry Point Specification, Version 2.1," EMVCo, Mar. 2011, pp. 1-50.
Etherington, "Android Pay Is Real, And Will Give Developers The Reins As An API," TechCrunch, https://techcrunch.com/2015/03/02/android-pay-is-real-and-will-give-developers-the-reins-as-an-api, Mar. 2, 2015, pp. 1-7.
"PCI DSS Version 2.0 Information Supplement: PCI DSS Tokenization Guidelines," PCI Security Standards Council, pcisecuritystandards.org, https://listings.pcisecuritystandards.org/documents/Tokenization_Guidelines_Info_Supplement.pdf., v 2.0, Aug. 2011, pp. 1-23.
"EMVCo Updates Payment Tokenisation Specification to Introduce 'Payment Account Reference,'" www.emvco.com, Mar. 29, 2016, pp. 1-2.
"EMVCO Publishes Technical Framework for its Payment Tokenisation Specification," EMVCO, Mar. 11, 2014, pp. 1-2.
"Encryption and Tokenization: Which is best for your business?," Townsend Security, 2010, pp. 1-4.
Molen, "Engadget Primed: What is NFC, and why do we care?," Engadget, Jun. 10, 2011, pp. 1-11.
"Exploring Google Wallet using the secure element interface," nelenkov.blogspot.com, Aug. 27, 2012, pp. 1-11.
"Financial Cryptography," 5th International Conference, FC 2001 Proceedings, Grand Cayman, British West Indies, Feb. 19-22, 2001, Paul F. Syverson (Editor), pp. 1-57.
"Gemalto to Provide Isis Mobile Commerce Platform with Trusted Service Manager (TSM) Solution," Business Wire, Dec. 12, 2011, pp. 1-3.
"Google Checkout checks out, replaced by Google Wallet," Android Community, Nov. 17, 2011, p. 1.
"Google Checkout HTML API Short Attribute Reference," Google Checkout, Google Code (archive.org), Mar. 27, 2012, pp. 1-4.
"Google Commerce: Building one wallet: Google Checkout is transitioning to Google Wallet," commerce.googleblog.com, Nov. 16, 2011, pp. 1-2.
"Google Prepaid Cards," Wallet Help, Google (archive.org), Oct. 3, 2012, p. 1.
Clark, "Google Unveils first Android NFC phone—but Nexus S is limited to tag reading only for now," NFC World, Dec. 7, 2010, pp. 1-4.
"Google Wallet launches officially on Nexus S 4G," Android Community, Sep. 19, 2011, pp. 1-2.
Garside, "Google Wallet mobile payments system launched to public," The Guardian, Sep. 19, 2011, p. 1.
Boulton, "Google Wallet Mobile Payments Coming to New York, Francisco; Google Wallet will launch this summer to enable consumers to pay for goods by tapping their Samsung Nexus 2 4G Android phones at NFC-fitted sales terminals at Subway, Macy's and other retailers," eWeek.com, May 26, 2011, pp. 1-2.
Fingas, "Google Wallet reaches the web, reminds most of us that it exists," Engadget, Oct. 4, 2012, pp. 1-6.
Raphael, "Google's Eric Schmidt spills clues about Android Gingerbread," ComputerWorld, Nov. 15, 2010, pp. 1-3.
"Handset makers line up behind Isis NFC payment platform," Old GigaOm, Sep. 27, 2011, pp. 1-2.
"How it Works," Wallet Help, Google (archive.org), Mar. 12, 2013, p. 1.
"How to find out IMEI number on Google Nexus S phone," Tech Notes Desk, Jan. 10, 2013, p. 1.

(56) **References Cited**

OTHER PUBLICATIONS

"La Caixa," Annual Report, 2010, Barcelona, Spain, pp. 1-190.
"Inside Contactless to Equip KTFMobile Payment Project Mobile Phones; Korean Manufacturer Confirms Inside's NFC Maturity by Embedding MicroRead into LG Electronics and Samsung Electronics Mobile Phones for its Mobile Payment Project," Business Wire, Jul. 16, 2007, pp. 1-2.
Cluckey, "Is a contactless ATM inevitable? Bank of America seems to think so; the FI has filed a patent application tor a 'Contactless Automated Teller Machine,'" ATM Marketplace, Sep. 20, 2012, pp. 1-3.
"Isis™ Launches in Austin and Salt Lake City; As Many as 20 Isis Ready™ Handsets to Be Available by Year End," Business Wire, Oct. 22, 2012, p. 1.
Perez, "Isis Revealed: Carrier-Led Mobile Payments Venture Shows Off Its New App, Announces Banking Partners," TechCrunch, Feb. 27, 2012, pp. 1-6.
Sadewo, "Isis to officially launch on Oct. 22, more supported devices announced," androidauthority.com, Oct. 18, 2012, pp. 1-2.
"MasterCard Approves NFC Phones from HTC, Intel, LG Electronics, Nokia, RIM, Samsung Electronics and Sony," Professional Services Close-Up, May 10, 2012, Close-Up Media, Inc., pp. 1-2.
"Mastercard Inc, Form 10-K (Annual Report)," Filed Feb. 28, 2007, for the Period Ending Dec. 31, 2006, pp. 1-204.
"MasterCard, Visa and American Express Propose New Global Standard to Make Online and Mobile Shopping Simpler and Safer," Global Hub, Engagement Bureau, Press Release, Oct. 1, 2013, pp. 1-2.
"Fact Sheet: Mobile Commerce: A New Way to Pay: MasterCard Mobile Commerce," May 26, 2011, pp. 1-4.
"McDonald's testing e-payment system," USA Today, May 29, 2001, pp. 1-3.
"Mobile Contactless Payments Trialled Live at Mobile World Congress 2010; GSMA, Samsung, Telefonica and Visa, with Giesecke & Devrient, Ingenico, ITN International and La Caixa, collaborate across industries to give Congress attendees an opportunity to experience NFC," Business Wire, Feb. 15, 2010, pp. 1-3.
"Mobile Payment Bringing value to payments on mobile," Gemalto, Nov. 2011, pp. 1-4.
Woo, "Mobile PayPass Meets Cloud in Google Wallet," Global Hub, Aug. 1, 2012, pp. 1-2.
Heun, "Mobile Wallet Consortium Strives Cautiously In 2012; The telco joint effort proceeded more slowly than expected, but its leaders maintain that the mobile wallet business is big enough for lots of players," Section: Mobile ISIS, Jan. 1, 2013, p. 47, vol. 2, No. 1, SouceMedia LLC d/b/a Arizent, pp. 1-3.
Bell, "Mobile's Gains Prompt More Banks To Move Beyond Cards For ATM Access," Payments Source, Section: Debit: vol. 1, No. 1, May 12, 2011, pp. 1-4.
"Standing Document (SD1): WG8 Projects: ISO/IEC 14443, Proximity Cards (PICCS)," ISO/IEC JTC1/SC17/WG8 (archive.org), Oct. 25, 2010, pp. 1-6.
"Telefonica O2 Czech Republic prepares NFC payments," DmEurope, Mar. 25, 2011, p. 1.
Markkanen, "Telefonica, Samsung to Pilot SIM-Based NFC Payment Solution in Spain," IHS Global Insight, Feb. 15, 2010, pp. 1-2.
"The Mobile Payments and NFC Landscape: A U.S. Perspective," Smart Card Alliance, Sep. 2011, pp. 1-53.
"Tokenization Guidance: How to reduce PCI compliance costs, Version 1.0," Securosis, Dec. 10, 2011, pp. 1-31.
"Tokenization: What's Next After PCi," RSA, 2012, pp. 1-8.
Seifert, "Verizon won't offer Google Wallet for the Galaxy Nexus because it uses a 'secure element'," The Verge, Dec. 10, 2012, pp. 1-2.
"Visa and Google Sign Licensing Deal to Boost Mobile Payment Adoption," Visa, Sep. 19, 2011, pp. 1-2.
"Visa Best Practices for Tokenization Version 1.0," Visa, Jul. 14, 2010, pp. 1-4.
Crosman, "Visa Certifies BlackBerry, Samsung And LG Phones For PayWave NFC Payments," Payments Source, Jan. 10, 2012, pp. 1-2.
"Visa Completes Acquisition of Rambus Payments Portfolio," Business Wire, Oct. 22, 2019, p. 1.
"Convenience for customers. Profits for you," Visa PayWave (archive.org), Jan. 2013, pp. 1-2.
"Verizon User Manual: Samsung Galaxy SIII," Verizon, Jan. 2012, pp. 1-204.
"World leader in proven and efficient cards for EMV deployment," Gemalto, Feb. 2010, pp. 1-2.
Becker, "29C3: A Rambling Walk Through an EMV Transaction (EN)," YouTube, https://www.youtube.com/watch?v=VdNm9JJmCzg, Dec. 30, 2012, pp. 1-2.
"ARQC and ARPC Generation and Validation," YouTube, https://www.youtube.com/watch?v=I1XTn175FFk, Paragon Application Systems, Jul. 25, 2012, pp. 1-3.
"CardVault by 3Delta Systems—Securing Credit Card Payments for B2B and B2G through Tokenization," YouTube, https://www.youtube.com/watch?v=h3zuiLiF51k, Feb. 1, 2010, pp. 1-3.
"CardVault by 3Delta Systems—Securing Credit Card Payments for B2B and B2G through Tokenization," Transcript of YouTube, https://www.youtube.com/watch?v=h3zuiLiF51k, Feb. 1, 2010, pp. 1-3.
"Credit Card Processing with EPX BuyerWall Tokenization," YouTube, https://www.youtube.com/watch?v=_7E5hj9li4g, Dec. 21, 2010, pp. 1-3.
"Credit Card Processing with EPX BuyerWall Tokenization," Transcript of YouTube, https://www.youtube.com/watch?v=_7E5hj9Ii4g, Dec. 21, 2010, pp. 1-7.
"Find out how PayPal works," YouTube, https://www.youtube.com/watch?v=dn42Y-2uFQM, Mar. 14, 2012, pp. 1-2.
"Google checkout," YouTube, https://www.youtube.com/watch?v=-UeYkxePW2c, Jun. 29, 2006, pp. 1-2.
"See Google I/O 2011: Google Checkout: A Foundation For Payments," YouTube, https://www.youtube.com/watch?v=7ts7Lkykn0E, May 13, 2011, pp. 1-2.
"See Google I/O 2011: Google Checkout: A Foundation For Payments," Transcript of YouTube, https://www.youtube.com/watch?v=7ts7Lkykn0E, May 13, 2011, pp. 1-64.
"Google I/O 2011: Howto NFC," YouTube, https://www.youtube.com/watch?v=49L7z3rxz4Q, May 10, 2011, pp. 1-2.
"Google I/O 2011: How to NFC," Transcript of YouTube, https://www.youtube.com/watch?v=49L7z3rxz4Q, May 10, 2011, pp. 1-62.
"Google I/O 2012: Introducing Google Wallet Cloud APIs," YouTube, https://www.youtube.com/watch?v=tpEGuSwv1fY, Jun. 29, 2012, pp. 1-3.
"Google I/O 2012: Introducing Google Wallet Cloud APIs," Transcript of YouTube, https://www.youtube.com/watch?v=tpEGuSwv1fY, Jun. 29, 2012, pp. 1-40.
"Google Nexus S by Samsung at CES 2011," YouTube, https://www.youtube.com/watch?v=5ZjtXH9S9KM, Jan. 11, 2011, pp. 1-2.
"Google Nexus S by Samsung at CES 2011," Transcript of YouTube, https://www.youtube.com/watch?v=5ZjtXH9S9KM, Jan. 11, 2011, pp. 1-2.
"Google Payments Live—Google Wallet updates," YouTube, https://www.youtube.com/watch?v=1pxkQ1mFjNA, Aug. 23, 2012, pp. 1-2.
"Google Payments Live—Google Wallet updates," Transcript of YouTube, https://www.youtube.com/watch?v=1pxkQ1mFjNA, Aug. 23, 2012, pp. 1-40.
"Google Wallet Demonstration," YouTube, https://www.youtube.com/watch?v=6tBAB5Is5vM, May 26, 2011, pp. 1-2.
"Google Wallet Demonstration," Transcript of YouTube, https://www.youtube.com/watch?v=6tBAB5Is5vM, May 26, 2011, pp. 1-2.
"Google Wallet Hands-On—Engadget," YouTube, https://www.youtube.com/watch?v=5s9wYEkRAgs, May 26, 2011, pp. 1-3.
"Google Wallet—How to Setup and Use this Exciting NFC Technology," YouTube, https://www.youtube.com/watch?v=_ay1FfLCsHs, Jul. 26, 2012, pp. 1-3.
"Google Wallet—How to Setup and Use this Exciting NFC Technology," Transcript of YouTube, https://www.youtube.com/watch?v=_ay1FfLCsHs, Jul. 26, 2012, pp. 1-7.
"Google Wallet Make Your Phone Your Wallet by Google," YouTube, https://www.youtube.com/watch?v=qRVQTQIJV0g, Feb. 18, 2013, pp. 1-2.

(56) **References Cited**

OTHER PUBLICATIONS

"Google Wallet Make Your Phone Your Wallet by Google," Transcript of YouTube, https://www.youtube.com/watch?v=qRVQTQIJV0g, Feb. 18, 2013, p. 1.
"Google Wallet Product Launch," YouTube, https://www.youtube.com/watch?v=am8t6iZ7up0, May 27, 2011, pp. 1-3.
"Google Wallet Product Launch," Transcript of YouTube, https://www.youtube.com/watch?v=am8t6iZ7up0, May 27, 2011, pp. 1-56.
"Google Wallet Walkthrough," YouTube, https://www.youtube.com/watch?v=xmbRSXYdFFs, Feb. 13, 2012, pp. 1-2.
"How does Google Wallet work? Really well!," YouTube, https://www.youtube.com/watch?v=jY2p-pNkjHA, Dec. 7, 2011, pp. 1-2.
"How does Google Wallet work? Really well!," Transcript of YouTube, https://www.youtube.com/watch?v=jY2p-pNkjHA, Dec. 7, 2011, pp. 1-2.
"How Does PayPal Work?," YouTube, https://www.youtube.com/watch?v=MdrPOCCFQ2k, Jul. 24, 2012, pp. 1-2.
"How To Use Google Wallet On Android," YouTube, https://www.youtube.com/watch?v=6DeiEVBIBcs, Oct. 28, 2011, pp. 1-2.
"How To Use Google Wallet On Verizon Galaxy Nexus—Pocketnow," YouTube, https://www.youtube.com/watch?v=AZ8t757ZfUs, Apr. 20, 2012, pp. 1-2.
Motorola MotoACTV Smartwatch, http://www.manualplanet.com/pdf/watches/motorola/motorola-motoactv-gpsfitness-tracker-quick-start-guide pdf, 2012, pp. 1-2.
Perez, "New NFC-Enabled Phones to Hit Europe," ReadWriteWeb, Feb. 18, 2011, pp. 1-3.
Wester, "New Samsung Galaxy S4 phone includes NFC, innovative barcode technology; New Samsung smartphone adds a number of features that may spur mobile payment adoption," Mobile Payments Today, Mar. 15, 2013, Networld Media Group, pp. 1-2.
"NFC Focus: Which Smartphones Have NFC?," International Business Times News, Aug. 9, 2012, pp. 1-3.
"NFC for mobile operators; Maximizing opportunities in the mobile NFC marketplace," Gemalto, Nov. 2009, pp. 1-2.
Cathelinais, "Nice, the first city to switch to contactless payment," 01net.com, May 21, 2010, pp. 1-6.
Clark, "Orange to offer Samsung Wave 578 NFC across Europe—but not in the UK," NFC World, Feb. 14, 2011, pp. 1-4.
Clark, "Orange to roll out NFC services across Europe in 2011," NFC World, Dec. 16, 2010, pp. 1-3.
"PayPal Credit Card Tokenization Extension—Magento Connect," Magento Extension Marketplace, http://www.magentocommerce.com/magentoconnect/catalog/product/view/id/18715/s/paypal-credit-card-tokenization-extension-4490/, Oct. 5, 2013, p. 1.
Nanninga, "PayPal Credit Card Tokenization in Magento," SitePoint, Sep. 30, 2013, pp. 1-11.
"Payment Card Industry (PCI), Data Security Standard, PCI DSS Applicability in an EMV Environment, A Guidance Document, Version 1," PCI Security Standards Council, Oct. 5, 2010, pp. 1-12.
"Standard: PCI PIN Transaction Security Point of Interaction Security Requirements (PCI PTS POI), Version: 1.0, Information Supplement: ATM Security Guidelines," PCI Security Standards Council, Jan. 2013, pp. 1-44.
"PayPal NVP API Developer Reference Enterprise Edition—eBay," Aug. 28, 2012, pp. 1-382.
"Rambus' Bell ID to support Android Pay," Rambus, Feb. 18, 2016, p. 1.
"RIM implements Bell ID's Token Manager software for mobile payments," WMI Company News, Jan. 23, 2013, World Market Intelligence Private Ltd., p. 1.
Lai, "Samsung and Visa join forces to enable NFC mobile payment at 2012 Olympics," Engadget, Apr. 1, 2011, pp. 1-6.
"Samsung and Visa Showcase Mobile Payments at the London 2012 Olympic and Paralympic Games," Business Wire, May 9, 2012, pp. 1-4.
Warren, "Samsung and Visa Take NFC Mobile Payments Global," Mashable.com, Feb. 25, 2013, pp. 1-2.
Haselton, "Samsung and Visa team up for NFC mobile payments at London 2012 Olympics," Boy Genius Report, Mar. 31, 2011, pp. 1-3.
"Samsung and Visa to Showcase Mobile Payments @ the London Olympics," Samsung Global Newsroom, May 9, 2012, pp. 1-3.
"Samsung Announces Launch Dates for Groundbreaking Mobile Payment Service: Samsung Pay," Samsung Global Newsroom, Aug. 14, 2015, pp. 1-2.
Grotta, "Samsung Begins to Phase Out Support of MST for Samsung Pay," Payments Journal, Feb. 22, 2021, pp. 1-3.
Murph, "Samsung cooks up its own NFC module, destined for the Nexus S?," Engadget, Dec. 1, 2010, pp. 1-2.
Molen, "Samsung Galaxy S III for Verizon Wireless review," Engadget, Jul. 9, 2012, pp. 1-10.
Trenholm, "Samsung Galaxy S3 is Olympic phone for no-touch payments," CNET, May 9, 2012, pp. 1-2.
"Samsung Google Nexus S—Full Phone Specifications, Reviews: Royal droid," GSMArena.com (archive.org), Nov. 2010, pp. 1-2.
"Samsung Google Nexus S review: Royal droid," GSMArena.com (archive.org), Feb. 11, 2011, pp. 1-2.
"Samsung partners with FeliCa for Japanese NFC solutions, unveils 2012 Olympics' mobile payment app with Visa," Engadget, Feb. 24, 2012, pp. 1-3.
Clark, "Samsung picks NXP for S3," NFCW, May 14, 2012, pp. 1-2.
"Samsung to Acquire LoopPay, Transformative Digital Wallet Platform," Samsung US Newsroom, Feb. 18, 2015, pp. 1-2.
Heun, "Samsung to Unveil NFC Smartwatch—Has Wrist-Payments' Time Come?," Payments Source, Sep. 2, 2013, SourceMedia LLC d/b/a Arizent, pp. 1-2.
"Samsung's New Secu-NFC Chip Enables Secure Mobile Payment by Enhancing NFC with Security Features," Plus News, Nov. 30, 2011, pp. 1-2.
Nanninga, "Save Credit Cards in Magento with Our New Paypal Extension," Classy Llama, Aug. 15, 2013, pp. 1-4.
"Shift4 Releases New Technology to Insure the Security of Its Merchants' and Partners' Payment Processing," Hotel Online (archive.org), Oct. 5, 2005, pp. 1-2.
"S-Pay: What is MST?," Samsung Levant, Sep. 22, 2020, pp. 1-2.
Susan Pandy, "Securing Payments: Payments Tokenization in Primetime," Federal Reserve Bank of Boston Payments Symposium, Jan. 20, 2016, pp. 1-20.
"Summary of ANS X9.119—Part 2 Use of Tokens To Protect Sensitive Card Data," Sep. 2017, pp. 1-2.
Marianne Crowe et al., "Is Payment Tokenization Ready for Primetime?," Jun. 11, 2015, pp. 1-51.
Terence Spies et al., "ANSI X9.119 Part 2: Using Tokenization Methods," 2013, pp. 1-20.
Assora et al., "A web transaction security scheme based on disposable credit card numbers," Int. J. Electronic Security and Digital Forensics, 2007, vol. 1, No. 2, Inderscience Enterprises Ltd., pp. 146-155.
Boyd, "A pragmatic approach to temporary payment cards numbers," Int. J. Electronic Security and Digital Forensics, 2009, vol. 2, No. 3, pp. 253-268.
Buccafurri et al., "Implementing disposable credit card numbers by mobile phones," Electronic Commerce Research, Feb. 23, 2011, vol. 11, Springer Publishing, pp. 271-296.
Javani et al., "A new credit card payment system based on 3D-Secure using one-time-use transaction numbers," Information Assurance and Security Letters, 2010, vol. 1, Dynamic Publishers, Inc., USA, pp. 060-065.
Killoran et al., "A New Secure Wireless Financial Transaction Architecture," EUROCON 2005, Nov. 22-24, 2005, IEEE, pp. 1060-1063.
Li et al., "A security-enhanced one-time payment scheme for credit card," Mar. 28-29, 2004, IEEE, pp. 1-11.
Mjølsnes et al., "On-Line E-Wallet System with Decentralized Credential Keepers," Mobile Networks and Applications, 2003, vol. 8, Kluwer Academic Publishers, The Netherlands, pp. 87-99.
Narayanaswami et al., "What Would You Do with a Hundred MIPS on Your Wrist?," RC 22057 (98634) Jan. 22, 2001, IBM Research, pp. 1-10.

(56) **References Cited**

OTHER PUBLICATIONS

Qasim et al., "Interactive Shopping with Mobile Wallet," World Congress on Sustainable Technologies, 2012, IEEE, pp. 32-36.
Honig, "A Week with Google Wallet," Endgadget, Sep. 19, 2011, pp. 1-49.
Kadambi et al.,"Near-Field Communication-Based Secure Mobile Payment Service," ICEC'09, Aug. 12-15, 2009, pp. 1-11.
"A closer look at Google Pay and tokenization," Rambus Press, Feb. 23, 2016, pp. 1-2.
Ghag et al., "A Comprehensive Study of Google Wallet as an NFC Application," International Journal of Computer Applications, Nov. 2012, vol. 58, No. 16, pp. 37-42.
"Add any credit or debit card," Google Wallet Help (archive.org), 2012, p. 1.
"Add any credit or signature debit card," Wallet Help, Google Wallet, Sep. 20, 2012, p. 1.
"Allynis Mobile NFC," Gemalto, Sep. 2007, pp. 1-4.
"Allynis TSM for Transport," Gemalto, Oct. 2009, pp. 1-2.
Adams, "Amex Plays a Major Role in Revamped Isis Mobile Wallet," Payments Source, Nov. 15, 2013, vol. 1, No. 1, SourceMedia LLC d/b/a Arizent, pp. 1-2.
Perez, "Android Pay, Google's Apple Pay Rival, Arrives Today," DigitalOcean, Sep. 10, 2015, pp. 1-8.
Heisler, "Apple Pay: An in-depth look at what's behind the secure payment system," Engadget, Oct. 2, 2014, pp. 1-7.
Fehr, "Apple Pay: How different is it from other Pay solutions, what role does tokenisation play, and to what degree can Card not Present payment benefit from Apple Pay in future," Technical Report RHUL-ISG-2018-3, Apr. 3, 2018, Egham, Surrey, UK, pp. 1-79.
"ATMIA publishes contactless ATM best practices," ATM Marketplace, Sep. 27, 2012, pp. 1-2.
Popper, "Banks Did It Apple's Way in Payments by Mobile," New York Times, Sep. 11, 2014, pp. 1-2.
"Bell ID Simplifies EMV Smart Card and NFC Application Management with Versatile New Platform," eBanking & Payment News, May 5, 2011, p. 1.
"BofA pursuing contactless ATM patent," Mobilepaymentstoday.com News, Sep. 20, 2012, Newstex LLC, pp. 1-2.
"Chip Advisory #20, Visa Recommended Practices for EMV Chip Implementation in the U.S," Jul. 11, 2012, pp. 1-10.
"Commbank, Mastercard and Samsung collaborate to launch NFC payment service," MarketLine NewsWire (Formerly Datamonitor), Dec. 13, 2013, pp. 1-2.
"Contactless Payment: Secure Enough?," Card Technology, Sep. 1, 2005, SourceMedia, Inc., Section: Special Issue: Contactless Technology, vol. 10, No. 8, p. 36.
"Eligible Devices," Google Wallet Help (archive.org), Nov. 18, 2012, p. 1.
Mott, "EMV and Mobile Payments, Questions abound, answers divide," Payments Summit Workshop, Feb. 4, 2013, pp. 1-22.
"EMV Integrated Circuit Card Specifications for Payment Systems Book 2 Security and Key Management Version 4.1," May 2004, pp. 1-187.
"EMV Integrated Circuit Card Specifications for Payment Systems. Book 2, Security and Key Management, Version 4.3," Nov. 2011, pp. 1-174.
"EMV Integrated Circuit Card Specifications for Payment Systems, Book 3, Application Specification, Version 4.3," Nov. 2011, pp. 1-230.

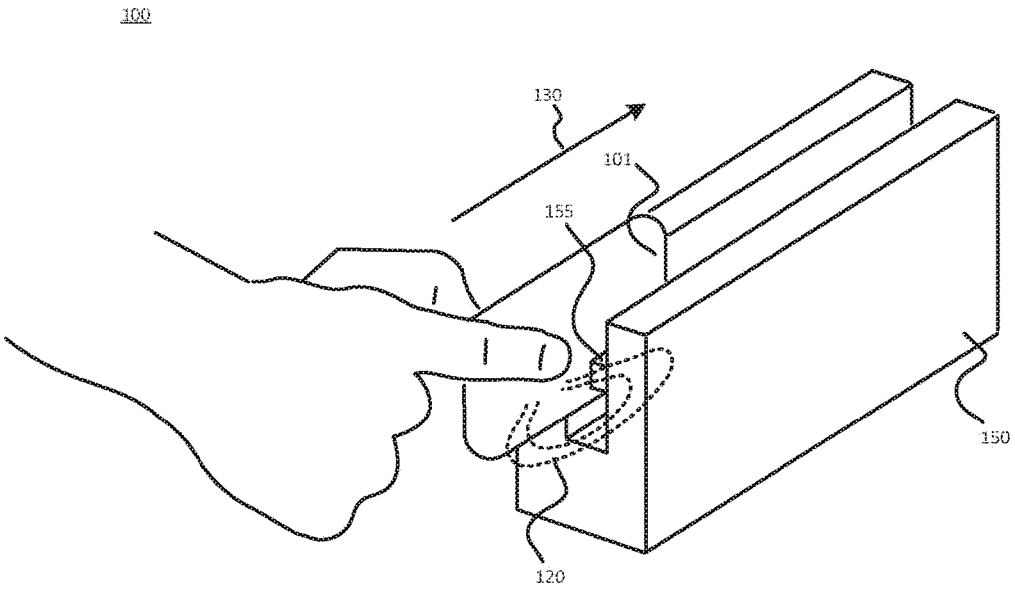


FIG. 1

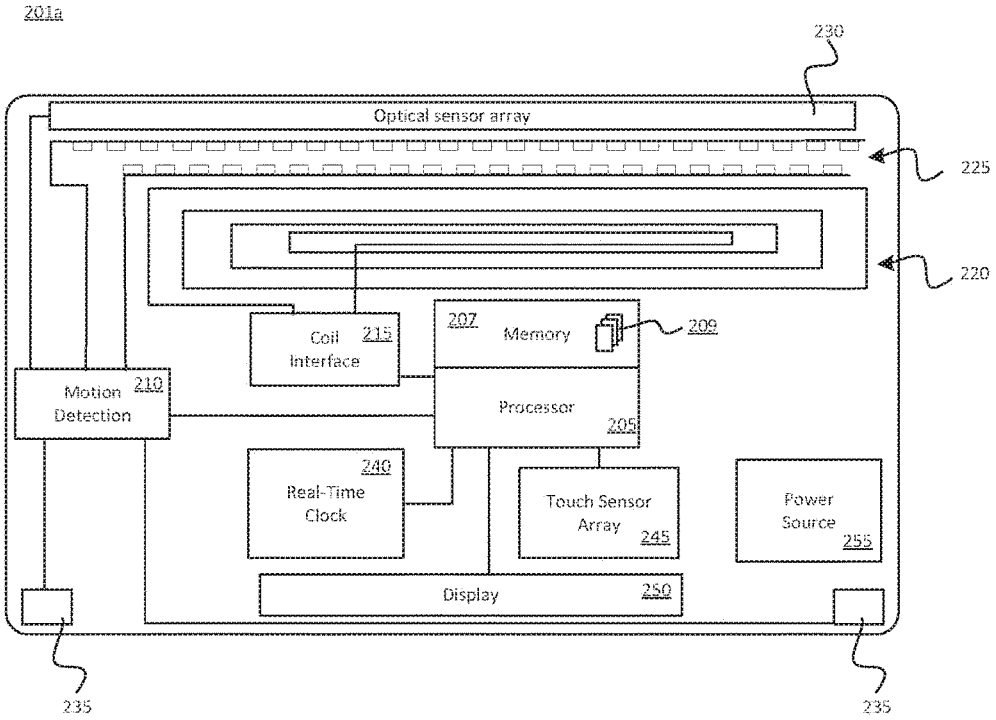

201a
230
Optical sensor array
225
220
Coil 215
Interface
207
Memory
209
Motion 210
Detection
Processor
205
240
Real-Time
Clock
Touch Sensor
Array
245
Power
Source
255
Display
250
235
235

FIG. 2A

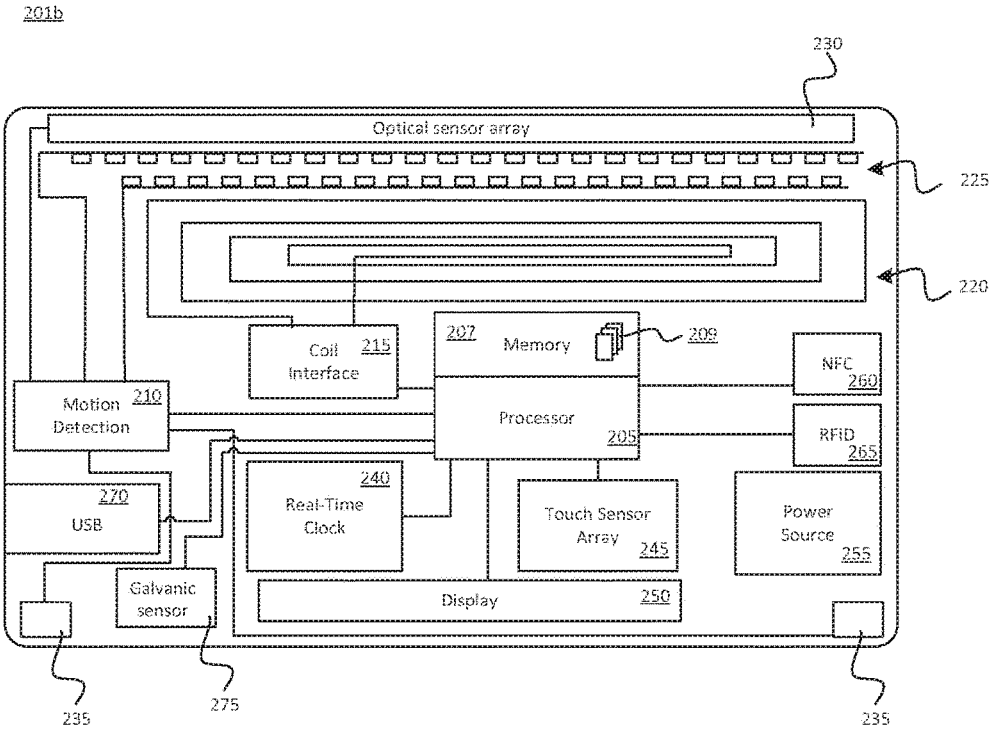

201b
230
Optical sensor array
225
220
Coil 215
Interface
207
Memory
209
NFC
260
Motion 210
Detection
Processor
205
RFID
265
270
USB
240
Real-Time
Clock
Touch Sensor
Array
245
Power
Source
255
Galvanic
sensor
Display
250
235
275
235

FIG. 2B

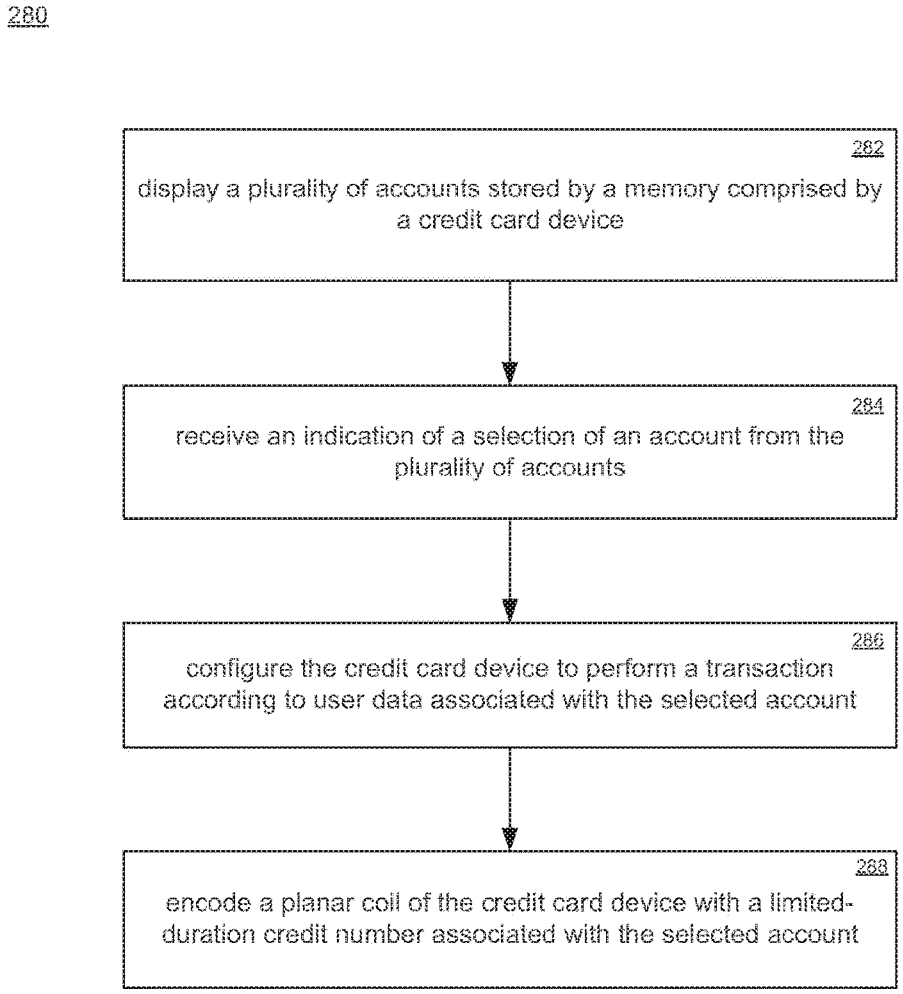

280
282
display a plurality of accounts stored by a memory comprised by a credit card device
284
receive an indication of a selection of an account from the plurality of accounts
286
configure the credit card device to perform a transaction according to user data associated with the selected account
288
encode a planar coil of the credit card device with a limited-duration credit number associated with the selected account

FIG. 2C

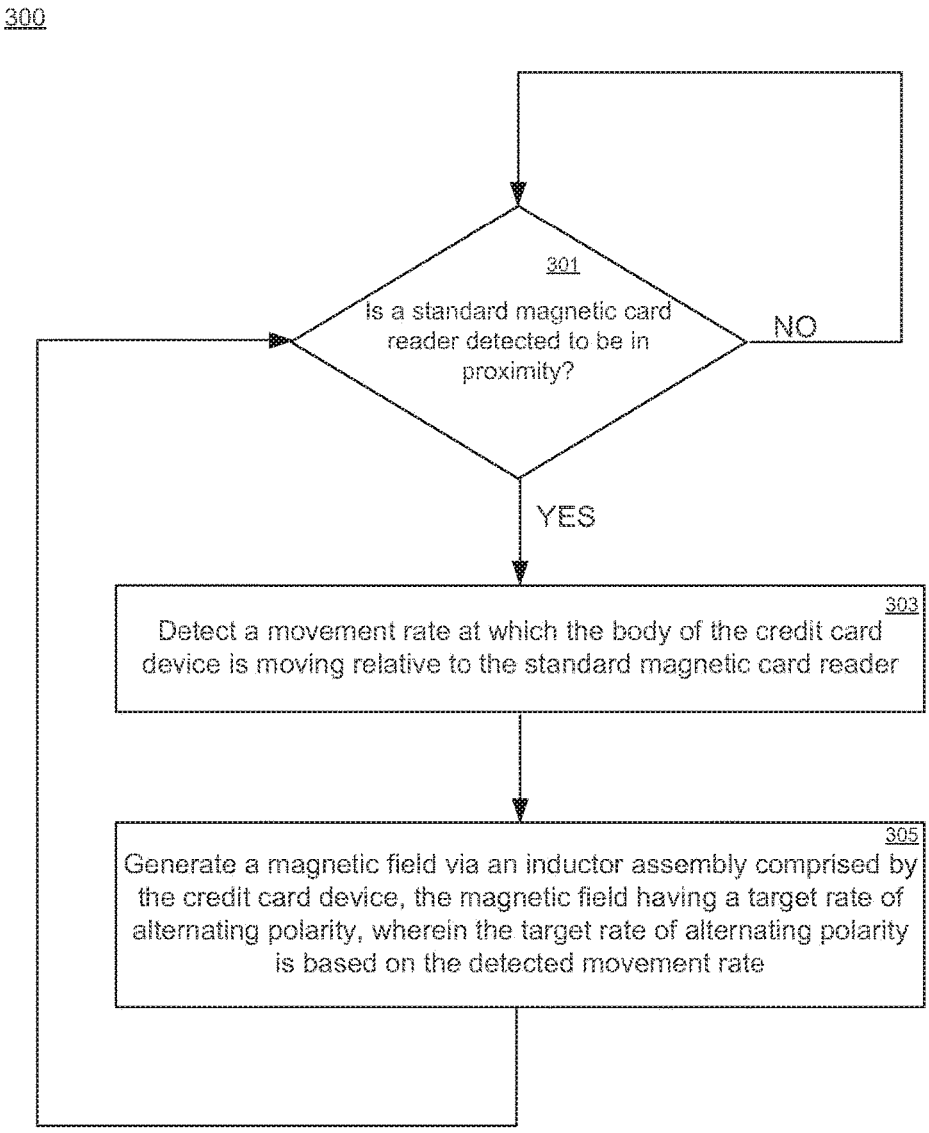

300
301
Is a standard magnetic card reader detected to be in proximity?
NO
YES
303
Detect a movement rate at which the body of the credit card device is moving relative to the standard magnetic card reader
305
Generate a magnetic field via an inductor assembly comprised by the credit card device, the magnetic field having a target rate of alternating polarity, wherein the target rate of alternating polarity is based on the detected movement rate

FIG. 3

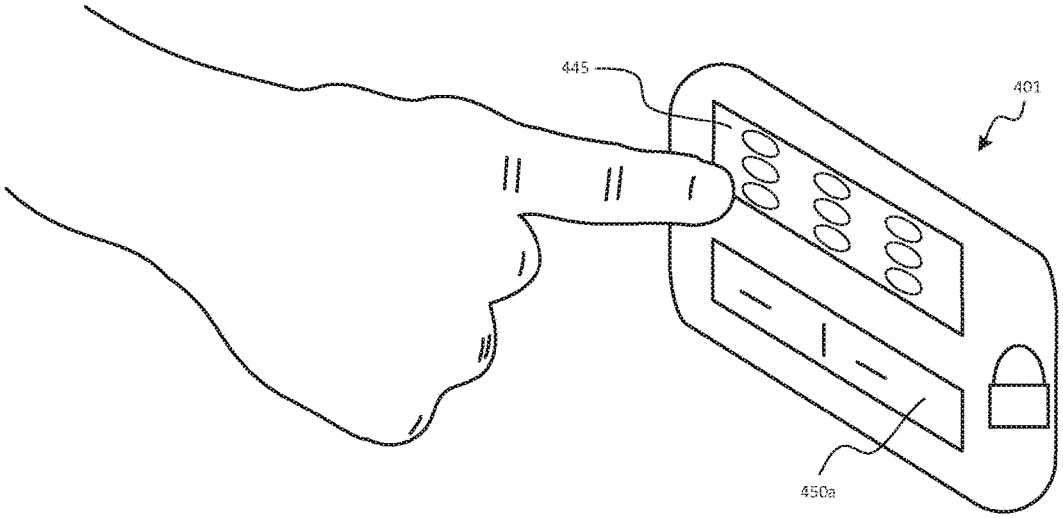


FIG. 4A

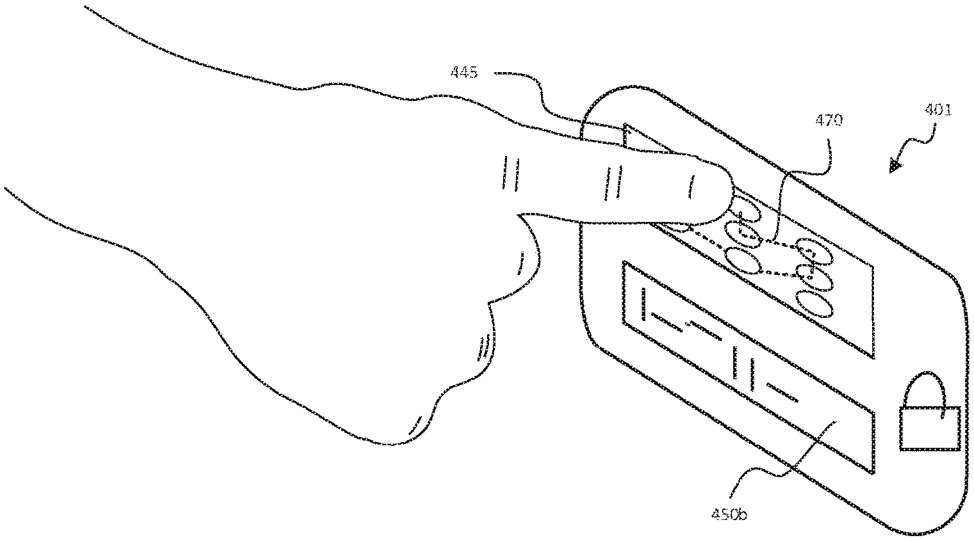


FIG. 4B

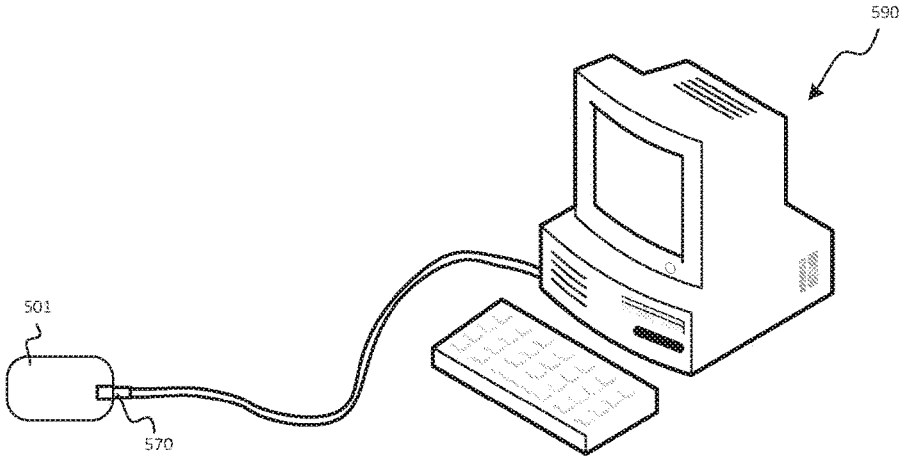


FIG. 5

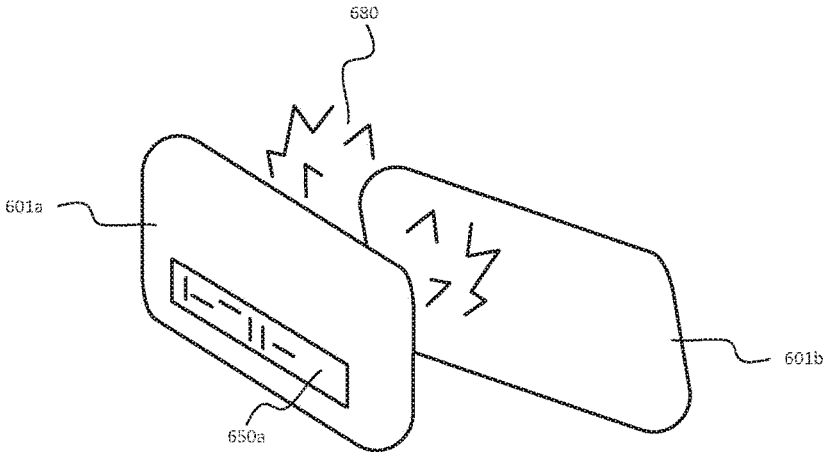


FIG. 6

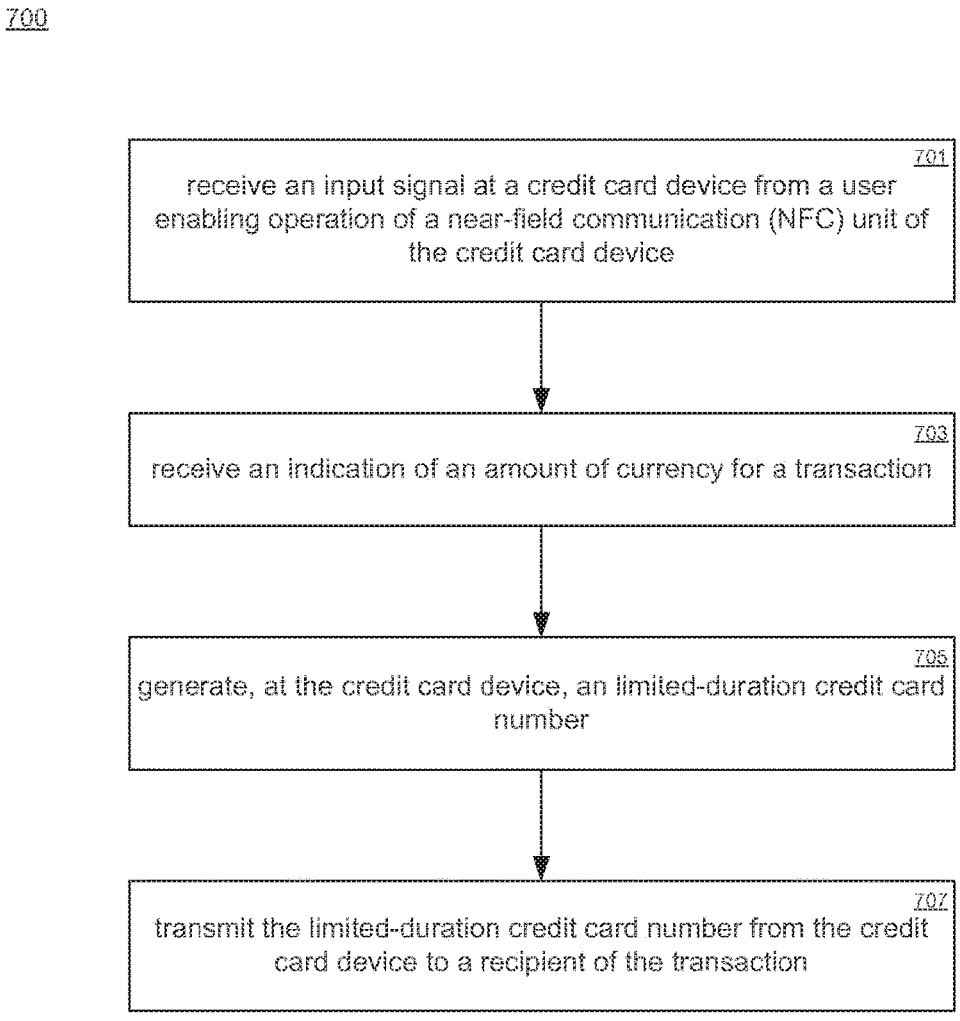

700
701
receive an input signal at a credit card device from a user enabling operation of a near-field communication (NFC) unit of the credit card device
703
receive an indication of an amount of currency for a transaction
705
generate, at the credit card device, an limited-duration credit card number
707
transmit the limited-duration credit card number from the credit card device to a recipient of the transaction

FIG. 7

MULTI-FUNCTION SMART TOKENIZING ELECTRONIC PAYMENT DEVICE

RELATED APPLICATIONS

This is a Continuation application of commonly-owned U.S. patent application Ser. No. 17/075,637, now U.S. Pat. No. 11,176,538, filed Oct. 2, 2020, which in turn was in turn a Continuation application of commonly-owned U.S. patent application Ser. No. 16/459,150, now U.S. Pat. No. 10,810,579, filed Jul. 1, 2019, which in turn was a Continuation application of commonly-owned U.S. patent application Ser. No. 15/701,261, now U.S. Pat. No. 10,339,520, filed Sep. 11, 2017, which in turn was a Continuation application U.S. patent application Ser. No. 14/981,757, filed Dec. 28, 2015, now U.S. Pat. No. 9,760,884, which in turn was a continuation of U.S. patent application Ser. No. 14/680,979, filed Apr. 7, 2015, now U.S. Pat. No. 9,224,083, which in turn was a Division of U.S. patent application Ser. No. 14/217,261, filed Mar. 17, 2014, now U.S. Pat. No. 9,022,286, which in turn claims priority from Provisional Application 61/794,891, filed Mar. 15, 2013, each of which are hereby incorporated herein in their entirety by reference.

FIELD OF THE INVENTION

Embodiments according to the present disclosure generally relate to electronic or smart payment devices and, more specifically, to more secure, smart multi-function smart tokenizing electronic payment devices and transaction processing thereof.

BACKGROUND OF THE INVENTION

There are several different types of credit cards available in the marketplace at present. A first type of credit card is a conventional, standard piece of plastic with a magnetic strip, which is readily available and in wide commercial use. The advantage of this first type of credit card is that a large portion of the infrastructure for credit card transactions is built around this type of card, and consequently such a card works in a wide array of vendors' credit card machines, automated teller machines (ATMs), and other devices that support the present credit card and banking infrastructure.

Another type of credit card device employs the use of a smart integrated circuit chip. These types of credit cards have a built-in microprocessor with cryptographic capabilities. These microprocessors operate in a similar manner to a cell phone having a chip comprising a cryptographic processor. Such a smart card device requires contact with a reader in order to be read and to perform a transaction. The reader provides the manner in which a facility interacts with the built-in processor on the card, e.g., for purposes of performing verification on the authenticity of the card or for making a direct deposit on the card. These credit card devices also comprise a magnetic strip such that they are compatible with standard plastic credit card readers in wide use.

A different type of credit card device in circulation employs radio frequency identification ("RFID"). These cards essentially have a low-power RF antenna built into the card, and when the cardholder passes the antenna in front of a reader comprising an RF field, enough power is generated to enable the processor to interact wirelessly with the receiving device.

A concern with each of these types of credit cards presently available in the marketplace is that they can all be, in various ways, susceptible to theft and/or compromise. Therefore, these types of credit cards have security limitations. Further, cards employing smart integrated circuit chips and RF technology are not in wide use at present because they are incompatible with existing credit card infrastructure, which still predominantly supports conventional plastic credit cards.

SUMMARY OF THE INVENTION

This Summary is provided to introduce a selection of concepts in a simplified form that are further described below in the Detailed Description. This Summary is not intended to identify key features or essential features of the claimed subject matter, nor is it intended to be used to limit the scope of the claimed subject matter.

An embodiment includes a multi-function electronic device capable of generating a programmed magnetic field of alternating polarity based on a speed of a card swipe, and methods for constructing the device for the purpose of emulating a standard credit card. An apparatus is described to allow said device to emulate behavior of a credit card when used in electronic credit card readers. Additionally, methods are described to allow user control of said device for the purpose of authorizing or controlling use of said device in the application of credit, debit and cash transactions, including cryptocurrency and device-to-device transactions. Methods are also described for generating a limited-duration payment number when performing a transaction for the purpose of creating a limited-use payment number, which is limited in scope of use to a predetermined number of authorized transactions. Furthermore, said device may interact with other similar devices in proximity for the purpose of funds or credit/debit transfers.

More specifically, an aspect of the present disclosure provides an apparatus comprising: a thin card shaped sized body; a memory operative to store a plurality of identification data; a processor coupled to the memory; a user interface for selecting a select identification data of said plurality of identification data; a magnetic card reader detection unit for determining if the body is adjacent to a standard magnetic card reader; and an inductor assembly coupled to the processor and integrated into the body, the inductor assembly under processor control for generating a magnetic field of alternating polarity responsive to the body being detected as adjacent to a standard magnetic card reader, the magnetic field generated in a region substantially encompassing the standard magnetic card reader, wherein the magnetic field encodes said select identification data, and wherein the magnetic field is operable to be read by a magnetic read head of the standard magnetic card reader.

According to another aspect of the present disclosure, a multi-function electronic device comprises: a near-field communication (NFC) unit; a touch sensor array; a display; a motion rate detection array; a memory, storing a user data and a currency amount; and a processor operatively coupled to the NFC unit, the touch sensor array, the display, the motion rate detection array, and the memory; and wherein the processor initiates a device-to-device transaction between two devices by a detected proximity of a first device and a second device and an input of information by a first user via said touch sensor array, and wherein the device-to-device transaction comprises an exchange of stored currency and said user data between the first device and the second device via the NFC unit.

According to yet another aspect of the present disclosure, a method of performing a transaction comprises: receiving

an input signal at a multi-function electronic device from a user enabling operation of a near-field communication (NFC) unit of the device; receiving an indication of an amount of currency for a transaction; generating at said device a limited-duration payment number; and transmitting said limited-duration payment number from said device to a recipient of the transaction.

BRIEF DESCRIPTION OF THE DRAWINGS

Embodiments of the present disclosure are illustrated by way of example, and not by way of limitation, in the figures of the accompanying drawings and in which like reference numerals refer to similar elements.

FIG. **1** is an illustration depicting an exemplary interaction between a device and a standard magnetic card reader, according to an embodiment of the present disclosure.

FIGS. **2**A-**2**B are block diagrams illustrating data flow between the magnetic coils on the device and the microprocessor on the device according to an embodiment of the present disclosure.

FIG. **2**C depicts an exemplary process of selecting an account from a plurality of stored accounts according to an embodiment of the present disclosure.

FIG. **3** is a flowchart illustrating an exemplary process of generating a magnetic field with an alternating polarity according to an embodiment of the present disclosure.

FIGS. **4**A-**4**B illustrate a user interacting with a touch sensor of a device, according to an embodiment of the present disclosure.

FIG. **5** is an illustration of a device connected with a computing system and operating according to an embodiment of the present disclosure.

FIG. **6** is an illustration of two devices performing a transaction according to an embodiment of the present disclosure.

FIG. **7** depicts an exemplary process according to an embodiment of the present disclosure.

DETAILED DESCRIPTION OF THE INVENTION

Reference will now be made in detail to the various embodiments of the present disclosure, examples of which are illustrated in the accompanying drawings. While described in conjunction with these embodiments, it will be understood that they are not intended to limit the disclosure to these embodiments. On the contrary, the disclosure is intended to cover alternatives, modifications and equivalents, which may be included within the spirit and scope of the disclosure as defined by the appended claims. Furthermore, in the following detailed description of the present disclosure, numerous specific details are set forth in order to provide a thorough understanding of the present disclosure. However, it will be understood that the present disclosure may be practiced without these specific details. In other instances, well-known methods, procedures, components, and circuits have not been described in detail so as not to unnecessarily obscure aspects of the present disclosure.

Some portions of the detailed descriptions which follow are presented in terms of procedures, steps, logic blocks, processing, and other symbolic representations of operations on data bits that can be performed on computer memory. These descriptions and representations are the means used by those skilled in the data processing arts to most effectively convey the substance of their work to others skilled in the art. A procedure, computer generated step, logic block, process, etc., is here, and generally, conceived to be a self-consistent sequence of steps or instructions leading to a desired result. The steps are those requiring physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical or magnetic signals capable of being stored, transferred, combined, compared, and otherwise manipulated in a computer system. It has proven convenient at times, principally for reasons of common usage, to refer to these signals as bits, values, elements, symbols, characters, terms, numbers, or the like.

It should be borne in mind, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to these quantities. Unless specifically stated otherwise as apparent from the following discussions, it is appreciated that throughout the present claimed subject matter, discussions utilizing terms such as "storing," "creating," "protecting," "receiving," "encrypting," "decrypting," "destroying," or the like, refer to the action and processes of a computer system or integrated circuit, or similar electronic computing device, including an embedded system, that manipulates and transforms data represented as physical (electronic) quantities within the computer system's registers and memories into other data similarly represented as physical quantities within the computer system memories or registers or other such information storage, transmission or display devices.

Encoding Via an Alternating Polarity of a Magnetic Field

In one embodiment of the present disclosure, a smart multi-function electronic device comprises a dynamic magnetic region (strip) incorporating a main inductor assembly from which programmed magnetic field data symbols are dynamically generated. In one embodiment the inductor assembly may be a planar coil formed within the material that embodies the multi-function electronic device. An advantage of using a planar coil is that it can dynamically produce a magnetic field in such a manner as to emulate the interaction between a traditional magnetic strip and a conventional card reader. As the magnetic strip of a conventional card is passed through a magnetic reader head, stripes of alternating magnetic polarity embedded in the strip induce a magnetic field of alternating polarity at the reader head. The pattern formed by the alternating polarity of the magnetic field encodes information, which when transformed by a transducer to a current signal in the magnetic reader head, provides user information for a transaction.

Embodiments of the present disclosure provide a multi-function electronic device able to generate a programmed magnetic field, wherein data is encoded and represented by an alternating polarity of the generated magnetic field. In a similar manner to a conventional plastic card, the magnetic field produced by the planar coil is able to be read by a pickup (or "transducer") and to thereby transmit information to the magnetic card reader. FIG. **1** illustrates a payment transaction **100** performed between a multi-function electronic device **101** and a conventional magnetic reader **150**. The multi-function electronic device **101** generates a magnetic field of alternating polarity **120** to be read by the conventional magnetic card reader **150**, according to an embodiment of the present disclosure. The multi-function electronic device **101** is moved at a rate **130** relative to a magnetic reader head **155** of conventional magnetic card reader **150**. The magnetic field **120** extends with sufficient distance and intensity from **101** so as to be read by magnetic

head reader **155**. The magnetic head reader **155** responds to the magnetic field **120** by producing a current in the conventional fashion, which is then interpreted as encoded information by the magnetic reader **150**. Therefore the magnetic field of alternating polarity **120** produced by the multi-function electronic device **101** has a substantially identical encoding effect as a traditional magnetic strip.

A characteristic of encoding information in a conventional magnetic card strip is that binary information is encoded by the pattern of alternating magnetic polarity formed by ferromagnetic stripes embedded on the magnetic strip. As the conventional magnetic card strip has a standardized format, the encoding of information is provided at a specified data density (bits per inch), according to which conventional magnetic readers are designed for interpretation of encoded data. In order to most ably emulate a conventional card interaction with a conventional magnetic reader the multi-function electronic device **101** of the present disclosure is provided with a means of determining a substantially optimal rate for alternating the polarity of the generated magnetic field **120** in order to produce data at a rate which is able to be readily received and correctly interpreted by the conventional magnetic reader **150**. Embodiments of the present disclosure provide several means of determining the relative movement rate **130** between the multi-function electronic device **101** and the magnetic reader head **155**. These features, as well as other characteristics of the multi-function electronic device of the present disclosure, can be better appreciated by a description of the internal components and functions of multi-function electronic device **101**.

FIGS. **2**A and **2**B depict exemplary embodiments of a smart multi-function electronic device, in a block diagram view. The components of the block diagram are illustrated according to functional connections, and their locations should not be construed as being limited to the respective locations as depicted in FIGS. **2**A-**2**B. In FIG. **2**A, multi-function electronic device **201***a* is shown in a block diagram view. Multi-function electronic device **201***a* comprises a processor **205** and a memory unit **207**, the processor **205** operatively coupled to the components of multi-function electronic device **201***a*. The memory **207** comprises a plurality of accounts **209**, which may be credit card accounts, banking accounts, merchant accounts, online accounts, cryptocurrency accounts, and combinations thereof. A motion detection module **210** is coupled to the processor unit **205** and to a set of motion detection units, which comprise a rate detection assembly **225**, an optical sensor array **230**, and a set of accelerometers **235**. The magnetic field is generated via a planar coil **220**, which is controlled by the processor unit **205** via a coil interface **215**. The rate at which the magnetic field changes polarity to encode the user data depends on the rate of relative movement detected by the rate detector. The multi-function electronic device **201***a* further comprises a real-time clock **240**, a touch-sensor array **245**, and a display **250**, each operatively coupled to the processor unit **205**. A user input may be made via the touch sensor array **245**, which may comprise a touch screen panel, a keypad, or a combination thereof. The display **250** is able to display an alphanumeric sequence, as well as graphical icons (such as a logo for a bank, or other images). Further, an optional backup power source **255** is depicted.

In one embodiment, the processor unit **205** is connected to the planar coil **220** and the motion detection units, via the motion detection module **210**. The processor unit **205** is responsible for determining the appropriate rate with which to output data from the planar coil **220**, wherein output data is encoded using alternating polarity of a generated magnetic field. The rate of the alternating polarity of the magnetic field is generated in accordance with the detected movement speed with which the card is swiped through the reader, in order for the reader to receive the encoded data at the appropriate rate. Magnetic card readers, which are designed to read conventional cards, are constructed to read data at specified input rates that correspond with the data density present in conventional magnetic card strips. The magnetic data symbols generated by the planar coil **220** are produced to align with the rate at which data is being read by the magnetic card reader. Accordingly, it is irrelevant if the multi-function electronic device **201***a* of the present disclosure is being swiped quickly or slowly, the planar coil **220** is controlled by the processor unit **205** to produce data at a substantially optimized rate, where the rate of data production is dependent on the rate at which the multi-function electronic device **201***a* is detected to be passing across the magnetic reader head.

FIG. **2**B depicts a multi-function electronic device **201***b* according to an embodiment of the present disclosure. Device **201***b* comprises a processor **205** and a memory unit **207**, the processor **205** operatively coupled to the components of multi-function electronic device **201***b*. The memory **207** comprises a plurality of accounts **209**, which may be credit card accounts, banking accounts, merchant accounts, online accounts, cryptocurrency accounts, and combinations thereof. A motion detection module **210** is coupled to the processor unit **205** and to a set of motion detection units, which comprise a rate detection assembly **225**, an optical sensor array **230**, and a set of accelerometers **235**. Additionally, a galvanic sensor **275** is coupled to processor unit **205**. The magnetic field is generated via a planar coil **220**, which is controlled by the processor unit **205** via a coil interface **215**. The rate at which the magnetic field changes polarity to encode the user data depends on the rate of relative movement detected by the rate detector. The multi-function electronic device **201***b* further comprises a real-time clock **240**, a touch-sensor array **245**, and a display **250**, each operatively coupled to the processor unit **205**. A user input may be made via the touch sensor array **245**, which may comprise a touch screen panel, a keypad, or a combination thereof. The display **250** is able to display an alphanumeric sequence, as well as graphical icons (such as a logo for a bank, or other images). Further, an optional backup power source **255** is depicted. Multi-function electronic device **201***b* further comprises a near-field communication (NFC) unit **260**, as well as a radio frequency identification (RFID) unit **265**, both of which are operatively coupled to the processor unit **205**. In one embodiment the NFC and RFID may share the planar coil for use as a radio frequency antenna, through the coil interface **215**. In one embodiment one or both the NFC and the RFID may have antennae dedicated to that individual sub-system. A universal serial bus (USB) connector **270** is coupled to the processor unit **205**. The functionality of the components with regard to exemplary uses of multi-function electronic devices **201***a* and **201***b* is described in greater detail in the following description.

A further aspect of the present disclosure provides a single multi-function electronic device that can be used for multiple banks or financial institutions. For example, instead of carrying a separate payment card for each account of a variety of payment card companies, a customer need only to carry a single device according to embodiments of the present disclosure. The capability of the multi-function electronic device to generate a multitude of payment numbers provides the ability of the multi-function electronic

device to be associated with multiple accounts. Furthermore, inputs at the touch sensor array on the multi-function electronic device can be used to select the appropriate bank or credit provider account stored in the memory unit of the multi-function electronic device.

FIG. **2**C depicts a process of selecting an account from a plurality of stored accounts in order to perform a transaction with the selected account, according to an embodiment of the present disclosure. The process **280** begins at step **282**, where a plurality of accounts stored by the multi-function electronic device memory is displayed. The plurality of accounts **209** are stored by memory **207**, and are displayed using display **250**. A user indicates an account selected from the plurality of accounts at step **284**. The selection is able to be made by keypad or touch sensor array **245**, and an indication of the selected account can be displayed via display **250**. At step **286** the multi-function electronic device is configured according to account information associated with the selected account, which may include an account number, an expiration date, and other user information associated with the account (e.g. a username, PIN, password, email address, etc.). At step **288** the planar coil of the multi-function electronic device is encoded with a limited-duration payment number that is associated with the selected account. The limited-duration payment number is able to be generated according to the selected account, a timestamp, a transaction amount, an indicated merchant, user key or secrets, on-card unique hardware secrets, payment authority key or secrets, user input from the card interface, and other information associated with the transaction.

Movement Rate Feedback

The relative movement rate of multi-function electronic device **201***a* is detected by one or more of the set of motion detection units, comprising the rate detection assembly **225**, the optical sensor array **230**, and the set of accelerometers **235**. Each of the motion detection units detects the motion of the device **201***a* in a distinct manner. The rate detection assembly **225**, which is positioned alongside (but independent of) the planar coil **220**, is able to detect the location of a magnetic head reader as the rate detection assembly **220** is being passed through the card reader. The reader module of a conventional card reader comprises a metal head having a small gap at the tip of the head. A pickup armature resides in this gap, such that as the metal head passes over a card strip, an electric field is induced in the head reader pickup circuit. In one embodiment the rate detection assembly **225** is constructed of an array of auxiliary inductor coils and magnetic pickup coils. As the metal head of the card reader assembly passes over the arrangement of auxiliary inductor coils and magnetic pickup coils of the rate detection assembly **225**, a disturbance in the magnetic field flowing between the two is induced, generating a change in current and producing a detected movement signal. The change in current is detected by the motion detection module **210**, and is used to determine the rate of motion of the card reader head passing across the surface of the multi-function electronic device **201***a* (and therefore along the planar coil **220**).

The optical sensor array **230** is also operable to detect a movement rate of the multi-function electronic device **201***a* with respect to a conventional magnetic card reader. The optical sensor array **230** is disposed nearby the planar coil **220**, in order to accurately detect a movement rate in the region of the planar coil **220**. In an embodiment, the optical sensor array **230** is a thin strip parallel to, and extending along, the length of the planar coil **220**. The optical sensor array **230** determines a location of a minimum of received light, which corresponds to the region of a surface in nearest proximity to the optical sensor array **230**. The magnetic reader head of a conventional magnetic card reader extends furthest from the surface of the card reader, and therefore the detected minimum in received light at the optical sensor array **230** corresponds with the location of the reader head. By tracking over time the position of this minimum received light along the optical sensor array, a detected movement rate may be found.

The set of accelerometers **235** are also operable to detect a movement rate of the multi-function electronic device **201***a*. The set of accelerometers **235** are positioned in the multi-function electronic device **201***a* in order to effectively measure the position and acceleration of the multi-function electronic device **201***a*. In an embodiment, the set of accelerometers comprises groups of accelerometers, each group having one or more accelerometers disposed at orthogonal planes to each other, and each group capable of generating signals that allow for determination of the orientation, motion and acceleration of the multi-function electronic device **201***a*.

The detected movement signal is received by the motion detection module **210**. The detected movement signal is generated by any one of the set of motion detection units, or any combination of motion detection units of the set. For example, the movement detection signal is able to be generated by the combination of the rate detection assembly **225** and the optical sensor array **230**. In an embodiment, the movement detection module **210** is able to determine the movement rate of the multi-function electronic device **201***a* from the detected movement signals, and transmits the determined movement rate, and orientation to the processor unit **205**. In an embodiment, the motion detection module **210** sends the detected movement signal to the processor unit **205**, and the processor unit **205** determines the relative movement rate.

In one embodiment, the generation of the magnetic field by the planar coil **220** at a specified rate of alternating polarity is accomplished according to the following description. One or more of the motion detection units in the set of motion detection units (rate detection assembly **225**, optical sensor array **230**, and set of accelerometers **235**) detect a movement rate of the multi-function electronic device **201***a* with respect to a magnetic card reader, and signal the motion detection module **210**. The movement rate is provided to the processor unit **205**, which determines the appropriate rate for alternating the polarity of the magnetic field generated by the planar coil **220**. The processor unit **205** outputs instructions or data to the coil interface **215** at the determined rate, which in an embodiment is a digital-to-analog converter (a DAC) and acts to translate the signal from digital to analog in order to drive the planar coil **220** and produce the magnetic field. The instructions from the processor unit **205** are comprise binary code, which are output through a shift register to the coil interface **215**. The shift register outputs data at a rate proportional to the determined movement rate of the multi-function electronic device **201***a*—thus, a higher determined multi-function electronic device **201***a* movement rate has a corresponding higher output rate at the shift register, leading to a higher rate of alternating polarity at the generated magnetic field (i.e., encoded data symbols output more quickly). Conversely, a lower movement rate of multi-function electronic device **201***a* leads the processor unit **205** to control the shift register to output data at a lower rate, and consequently the rate of alternating polarity in the generated magnetic field is lower.

FIG. **3** illustrates an exemplary process **300** for determining the rate to alternate the polarity of the generated magnetic field of the multi-function electronic device, according to an embodiment of the present disclosure. At step **301** the process determines if a standard magnetic card reader is detected to be in proximity with the multi-function electronic device. If NO, the step repeats. If YES, the process moves to step **303**. At step **303** a detection of a movement rate at which the body of the multi-function electronic device is moving relative to the standard magnetic card reader is made. The process continues at step **305**, wherein a magnetic field is generated by an inductor assembly comprised by the multi-function electronic device, the magnetic field having a target rate of alternating polarity that is based on the detected movement rate from step **303**. The process then repeats at step **301**, determining if a standard magnetic card reader is (or remains) in proximity to the multi-function electronic device. In this manner, while a standard magnetic card reader is detected to be in proximity to the multi-function electronic device, the movement rate of the multi-function electronic device is determined and the polarity and orientation of the generated magnetic field is alternated at the appropriate rate, to recreate the data as described above, at the correct rate, in order to clock out the data to be conveyed to the magnetic strip reader, at a rate matching the action of an ordinary magnetic strip card through same the magnetic card reader.

Security

Security is an area of concern for payment card holders, as the small form factor makes theft quite easy, and additionally there are many ways for a malicious third-party to record the account number of a payment card in order to later make fraudulent transactions on the account. Embodiments of the present disclosure address security concerns of a payment card owner on several fronts.

In one aspect, security of the multi-function electronic device is enhanced by providing a means of locking the multi-function electronic device in order to prevent use, until such time that a valid user input is entered. Embodiments of the present disclosure provide a multi-function electronic device having a region for receiving human input, e.g., touch sensors which are able to be formed by contacts that a user can press (e.g., the touch sensor array **245** of FIGS. **2**A-**2**B). FIGS. **4**A-**4**B illustrate a user interacting with a multi-function electronic device **401** via a keypad or touch sensor array **445**. In FIG. **4**A, the multi-function electronic device **401** is in a locked state. A display **450** is able to display a message to the user, for instance, the message "device locked" or "enter password," or question prompts which guide the user to respond with answers through the key-pad or the touch sensor, to certain preset questions, that confirm personal knowledge known only to the associated user. The touch sensor array **445** enables user interaction with the multi-function electronic device **401**. An exemplary use of the touch sensor array **445** is an input of a currency amount to be used in a transaction. The touch sensor array **445** is able to include buttons, or a touch-sensitive pad, or a combination of the two. Other embodiments of the touch sensor array **445** allowing a user to input data to the multi-function electronic device **401** are consistent with the spirit and scope of the present disclosure.

In order to unlock the multi-function electronic device **401** and enable a transaction or other usage, the user inputs data via the touch sensor array **445**. FIG. **4**B illustrates the user inputting a password via a gesture **470**, which operates to unlock the multi-function electronic device **401**. The display **450***b* is able to display a message indicating the multi-function electronic device **401** is unlocked and ready for use, for instance, display **450***b* may display the message "unlocked," or it may display an account number associated with the multi-function electronic device **401**.

Embodiments of the present disclosure provide additional functionality for the touch sensor array **445**. For example, there may be touch contact terminals that a user can press to wake up the multi-function electronic device **401**, to cause the battery to supply power, or to place the multi-function electronic device **401** in a power reduction mode when it is not being used. In an embodiment, if any number other than the correct password is entered multiple times, or if there is an attempted usage of the multi-function electronic device **401** without entering in a password, an automatic phone call may be triggered to the appropriate fraud protection authorities.

In one embodiment of the present disclosure, the display **450** is a thin-film liquid crystal display ("LCD"). The display **450** is able to have multiple uses. In one embodiment, the display **450** can be used to cue the user for a security question upon input of an improper password. Or if fraud protection services need to contact a customer, they can verify the customer's identity by transmitting a security question to the display **450** of user's multi-function electronic device **401**, to which the user would need to respond correctly using the input buttons of touch sensor **445** on the card.

Limited-Duration Payment Number

A further security feature of the multi-function electronic device provided in the present disclosure is the capability of producing a limited-duration payment number for performing transactions using accounts of the card. The multi-function electronic device comprises a real-time clock that is able to produce a cryptographically protected timestamp for each interaction. The power source is able to activate the processor unit such that a unique number may be generated by the multi-function electronic device and verified by the payment authority according to the timestamp and the transmitted user information. The limited-duration payment number is able to be produced at the time the multi-function electronic device is performing a transaction, and is able to be generated according to the user's private information, a bank information, information regarding the facility performing the transaction, and the time of day. The limited-duration payment number is able to be limited to only one transaction, a finite number of transactions, or may be limited to a specified period of time—e.g., 2 minutes, 10 minutes, 3 hours—after which time that particular limited-duration number would become invalid. As detailed above, if an expired limited-duration payment number is attempted to be used for a transaction, the transaction is denied and an automatic notification is able to be made to a payment authority in order to notify the user and to prevent transactions on the account. The transaction count is able to be determined through the action of passing the card through magnetic reader, and the process of transmitting the payment number to the card reader.

In one embodiment, the number on the front of the card is able to be a full or partial number. In an embodiment, the number displayed on the multi-function electronic device is a static number, but the number transmitted during a transaction is a limited-duration payment number as described above. The number displayed on the multi-function elec-

tronic device may not necessarily be a static number. For example, the first four and last four digits of the payment number are able to be fixed, while the remaining eight digits can be dynamically generated. As the device is read by the machine, part or all of the number may be dynamically produced at the time the device is read. As described above, the dynamic part of the limited-duration payment number generated may be based on the user's private information, the user's bank information, the time of day or the facility that is reading the card. Further, the expiration date of the multi-function electronic device can also be dynamically generated.

Effectively, embodiments of the present disclosure provide a multi-function electronic device that has no fixed number, as illustrated in FIG. **11**, and therefore the account cannot be compromised. Only the number generated at the instant of the multi-function electronic device transaction matters. Accordingly, unauthorized use of the multi-function electronic device is highly unlikely, because a transaction cannot be conducted with an expired limited-duration payment number, or only the static portion of the payment number. In one embodiment of the present disclosure, sufficient dynamically generated numbers are provided for on the multi-function electronic device such that a unique payment number can be generated for each transaction. In this embodiment, the multi-function electronic device of the present disclosure effectively acts as a unique per-transaction payment device.

With reference to FIG. **2**A, **2**B, in one embodiment, the process steps enabling a card transaction are as follows. A multi-function electronic device (e.g., multi-function electronic device **201***b*) is connected to a computer system (e.g. computer system **590**, FIG. **5**), via any of the connection means available to the multi-function electronic device (USB **270**, NFC **260**, and RFID **265**). User data and other essential information, such as account information, are downloaded to the multi-function electronic device. For example, for an account designed for online transactions, user account information will likely include an account email and an account password. The account may be for example a bank account, a credit account, a merchant account, an online transaction account, or a cryptocurrency. In one embodiment a currency amount is also downloaded, which is made accessible to the multi-function electronic device **201***b* for transactions. In an alternative embodiment, rather than a currency amount being downloaded to the multi-function electronic device **201***b*, the user account information (e.g., username and password) is stored such that a subsequent authorized multi-function electronic device **201***b* transaction is automatically pre-authorized to deduct (or credit) the entered transaction amount at a stored account. In an embodiment, a user uses the touch sensor array **245** of the multi-function electronic device **201***b* in order to input the user information, including the amount of currency to be stored. The information entered by the user is able to include an account source of a transaction (e.g., bank account, credit account, merchant account, ATM, online payment service, or a cryptocurrency), as well as a type of transaction to be made (e.g., as a debit card, as a credit card, or as a user account). In another embodiment, the information is entered using the computing system to which the multi-function electronic device **201***b* is connected.

Transactions may be authenticated on the specified account by entry of the username and password for the account during the transaction, using the touch sensor array **245**. In an embodiment, a password for an account is represented by a user input (such as a gesture, a swipe, and/or an unlock keycode) which is entered on multi-function electronic device **201***b* during a transaction for account authentication. According to an embodiment of the present disclosure, a user that has "primed" the multi-function electronic device **201***b* for a transaction has already performed a security authentication on the card, and therefore a subsequent card transaction is able to be pre-authorized to perform the transaction without further user authentication steps. The priming action can be a tap of the multi-function electronic device **201***b* detected by accelerometers **235**, or a gesture, swipe, or a key input received by touch sensor array **245**.

A transaction is able to be communicated using the planar coil **220**. In one embodiment, when the transaction is a payment transaction, a limited-duration payment number is generated. A user inputs an amount for the transaction using the touch sensor array **245**, and the limited-duration payment number is generated to correspond with the entered amount. The binary data corresponding to this limited-duration payment number is sent from the processor unit **205** to the coil interface **215**, where it is converted to an analog signal in order to drive the planar coil **220** to generate a magnetic field having an alternating polarity corresponding to the encoded data of the limited-duration payment number.

Online Transactions

FIG. **5** displays the multi-function electronic device **501** in connection with a computing device **590**. In one embodiment, the multi-function electronic device **501** is able to be used to make online purchases. In one embodiment, the multi-function electronic device **501** is equipped with a means **570** for communicating with the USB port on a computer or other device in order to make online purchases. In one embodiment the multi-function electronic device **501** may have an area cut out, such that contact terminals corresponding to a USB cable connector are contained within, enabling connection of a USB cable (e.g., a micro-USB connection). When performing online transactions, the multi-function electronic device **501** can uniquely generate a limited-duration payment number (as described above) for online purchases. The multi-function electronic device **501** receives a user input indicating that a transaction is imminent, and an authorization. The user input is able to comprise a gesture, a swipe, a key input sequence, and combinations thereof. The limited-duration payment number is able to be displayed on the front display of the multi-function electronic device **501**. In one embodiment, the multi-function electronic device **501** is able to use RFID **265** or near field communication NFC **260** technology in order to connect to a personal computer **590**. This enables a per-transaction, limited-use payment number, enhancing the security of the payment account by substantially negating the possibility of a theft of the payment number used to perform the transaction leading to account compromise. See also, for example, FIG. **10**.

According to an embodiment, the transaction is able to include information regarding a user account, such as an email address of the user, and upon reconnection of multi-function electronic device **201***b* to a computer system (for instance, computer system **590**), the transaction information stored on multi-function electronic device **201***b* could be "replayed" by the computer system in order to finalize the transaction.

In one embodiment, a means of limiting an available credit amount are provided. According to the download process described above, the multi-function electronic

device is able to have a total credit available. The multi-function electronic device is able to reference the total credit available in subsequent transactions, and will provide limited-duration payment numbers corresponding to amounts up to, but not exceeding, the remaining credit available to the multi-function electronic device. An attempt to perform a transaction having an amount exceeding the remaining credit available will not result in a valid limited-duration payment number, and therefore an authenticated transaction cannot proceed. In general, the multi-function electronic device will only successfully generate a limited-duration payment number if the proper conditions for a transaction are determined to be present. The proper conditions for a transaction comprise a correct identification having been made by the user (via a gesture, swipe, and/or key input) and an amount for the transaction indicated to be less than the total credit available to the account indicated for the transaction.

Device-to-Device Transactions

In addition to transactions performed using conventional magnetic card readers (such as at point-of-sale locations, banks, and automated teller machines (ATMs)) and via cable connection with a computing device, transactions performed wirelessly between a device and a device (e.g., card-to-card, card-to-computer device having a reader dongle, card-to-ATM) are provided according to embodiments of the present disclosure. See, for example, FIGS. **8** and **10**. For simplicity, the following describes a device-to-device transaction, but it will be understood that card-to-device transactions are similarly provided.

FIG. **6** illustrates a device-to-device transaction according to one embodiment. A first multi-function electronic device **601***a* comprises a display **650***a*, and is in contact with a second multi-function electronic device **601***b*. A contact interaction between the devices is indicated by interaction **680**. In one embodiment, the contact interaction is a tapping of a device **601***a* against another device **601***b*. In another embodiment, an optical sensor array at one or both of the devices detects interaction **680**. In another embodiment, interaction **680** indicates a swipe of a device **601***a* across another device **601***b*. In one embodiment a user input through the key-pad initiates and enables a transaction from first device to second device. In one embodiment the presence of second device in preparation for device-to-device transaction is confirmed through "polling", the process of which involves transmission of data between devices, and confirmed receipt of transmitted data by response received from second device received at first device, including information confirming receipt of the information, by second device.

The planar coil comprised by each of multi-function electronic device **601***a* and multi-function electronic device **601***b* is able to be a means of transferring information for a transaction, e.g., such as an antenna. Once either, or both, of multi-function electronic device **601***a* and multi-function electronic device **601***b* detect interaction **680**, a transaction is able to be completed via generation of a magnetic field at one card and reception of the magnetic field (i.e., reading) at the other card. In this manner, the device (e.g., multi-function electronic device **601***a*) receiving the transaction information operates its planar coil in an antenna mode. This enables multi-function electronic device **601***a* and multi-function electronic device **601***b* to authentically perform a transaction, and to transfer a currency between multi-function electronic device **601***a* and multi-function electronic device **601***b*. As described above, in an embodiment the transaction is able to use a limited-duration payment number to encode the transaction.

In an embodiment, a set of accelerometers is used to detect the beginning of the transaction, for instance, a transaction performed by a swipe of multi-function electronic device **601***a* across multi-function electronic device **601***b*. Further, the set of accelerometers can detect a "priming" action for a multi-function electronic device, i.e., an indication for a multi-function electronic device that a transaction is imminent. The priming action can be a tap of the multi-function electronic device **601***a*, or tapping the multi-function electronic device **601***a* against the multi-function electronic device **601***b*. In one embodiment, a touch sensor array is able to be used for the priming action.

In an embodiment of a device-to-device transaction, one device (e.g. **601***a*, the device of the user having a currency debit) generates the limited-duration payment number, which is transmitted via the device's planar coil. The multi-function electronic device of the recipient (e.g., **601***b*, the card of the user receiving a currency credit) receives the encoded data via the planar coil, acting as an antenna, and the coil interface is able to convert the received signal into a digital signal understood by the processor to be the limited-duration payment number, identifying both the correct account and the amount of the transaction.

In one embodiment, the multi-function electronic device **201***b* stores cryptocurrency information in processor unit **205**. The cryptocurrency information stored is able to include a plurality of cryptocurrency addresses, a plurality of private keys, and a plurality of public keys. The multi-function electronic device **201***b* is able to perform a transaction, as described above, using a cryptocurrency as the specified account. In one embodiment, the multi-function electronic device **201***b* is able to hash a portion of the transaction, using the processor unit **205** and the real-time clock **240** along with user information pertinent to the cryptocurrency account and the transaction. A subsequent connection of the device **201***b* to a computing device provides a means of connecting to the cryptocurrency servers and finalizing the transaction. Further, the multi-function electronic device **201***b* is able to sign a cryptocurrency transaction by, for instance, receiving a prompt at the display **250** to input a dynamic PIN specific to the transaction, which is able to be entered by touch sensor array **245**.

In a device-to-device cryptocurrency exchange, a record of the transaction can be made according to the following. A first device (e.g. **601***a*) making a deduction with an amount indicated via touch sensor array **245** is able to generate a record of the transaction and store the record in the device memory, while a second device (e.g. **601***b*) receiving the cryptocurrency is able to generate a confirmation of the received transaction amount. In one embodiment, the amount indicated is provided by the receiving device **601***b*. The hashed record of the transaction contains the unique information of each user, along with the transaction amount. The success or failure of the transaction is able to be displayed on the respective displays of devices **601***a* and **601***b*.

Account Theft and Unintended Use Prevention

A security concern for conventional credit cards utilizing wireless communication means is the ability of a thief to access and/or copy user information through un-detected interaction with the wireless communication means. Sensitive and confidential information can be gleaned via, for

example, "listening-in" on an RFID interaction between a credit card and a contactless reader, recording the characteristics of the interaction, and replicating certain characteristics to fake an authorized transaction. While to a great extent security concerns are addressed by the usage of limited-duration payment numbers and other security features provided for by the device of the present disclosure and previously described, a further security feature regarding the wireless communication means of the multi-function electronic device is described herein.

In one embodiment, wireless communication means of the multi-function electronic device **201***b* are in a powered-down, or disabled, state prior to receiving an authenticated activation signal from a user. Upon receiving the activation signal, the communication means (e.g., NFC **260**, RFID **265**, and planar coil **220**) are activated, enabling the multi-function electronic device **201***b* to conduct a transaction. The activation signal can originate from one (or a combination) of the set of motion detection units (rate detection **225**, optical sensor array **230**, and accelerometers **235**), the touch sensor array **245**, and the galvanic sensor **275**. The galvanic sensor **275** is operable to detect a contact of human skin, via a current produced at the sensor **275** upon such contact. See also, for example, FIG. **8**. In an embodiment the galvanic sensor **275** is comprised of metallic contacts disposed on opposite sides of, and isolated by, the body of multi-function electronic device **201***b*. In one embodiment, the current produced by user contact with the galvanic sensor **275** contacts is sufficient to provide small amounts of energy in order to power components of the card. For example, energy produced is able to power the processor unit **205** and the RFID **265**. In one embodiment the galvanic sensor **275** further comprises two conducting surfaces separated by a junction, and the galvanic sensor **275** is configured as a thermoelectric generator (e.g., via the Peltier effect, the Seebeck effect, or a combination). For example, heat applied at one surface of the multi-function electronic device **201***b* may lead to differential heating between the opposing, separated conducting surfaces of the galvanic sensor **275**, generating an electric current and powering a subset of, or all of, the components of multi-function electronic device **201***b* (e.g., the processor unit **205**, the NFC **260**, and the RFID **265**).

In an embodiment, the communication means are activated only so long as the activation signal continues to be detected. In another embodiment, the communication means are activated for a specified amount of time following detection of the activation signal. For example, if using the multi-function electronic device **201***b* in an ATM (or other device) preventing continuous human contact, the activation signal is able to be a swipe, gesture, or key input sequence entered via the touch sensor array **245**, which activates the device for a specified duration (for instance, one minute). In an embodiment the detection of motion through accelerometer input indicates activation by a valid user. In one embodiment the specific motion detected through accelerometer input corresponding with a specific user action, such as a "flick", "swipe", "spin", "wave", "tap," may be used to initiate activation, wherein the motion is not normally generated at idle and during periods of inactivity. For example the motion not being generated accidentally while the device is stored in a user's wallet, carried while the user is actively moving, or is being handed from user to a clerk at a point of transaction. In one embodiment the specific motion, or sequence of motions, may be associated with a user, and stored on the device memory, such that performing the correct sequence when prompted can confirm the possession of the device by the known owner, thus initiating activation and enabling usage.

FIG. **7** depicts a process of selectively enabling the communication capability of the multi-function electronic device according to an embodiment of the present disclosure. The process **700** begins at step **701**, where an input signal is received at the multi-function electronic device from a user. The input signal is able to be generated by any one, or combination, of a plurality of input means, where the input means comprise: a swipe gesture received at a touch sensor array; a key press sequence; an accelerometer sensor indication of multi-function electronic device motion; and a galvanic sensor indication that the device is in a user grasp. The input received from the user enables operation of a near-field communication (NFC) unit of the multi-function electronic device. In one embodiment, the NFC unit is disabled prior to receiving the input signal. In one embodiment, an RFID communication unit is disabled prior to receiving the input signal, and is activated by the input signal. In one embodiment, the planar coil is disabled prior to receiving the input signal, and is activated by the input signal.

The multi-function electronic device, following enablement of the NFC unit, receives an indication of an amount of currency for a transaction at step **703**. At step **705**, the multi-function electronic device generates a limited-duration payment number, which at step **707** is transmitted to a recipient of the transaction. In one embodiment, the limited-duration payment number has a limited recurrence, and is limited in scope of use to a predetermined number of authorized transactions.

In the foregoing description of process **700**, the ordering of the process steps is exemplary and should not be construed as limiting. Alternative ordering of the process steps is consistent with the present disclosure, as conceived by one skilled in the relevant art.

In one embodiment of the present invention, a credit card comprises a dynamic magnetic strip incorporating a main inductor assembly from which magnetic field data symbols are dynamically generated. In one embodiment the inductor assembly may be a planar coil formed within the plastic that the credit card is composed with. The advantage of using a planar coil is that it can produce the same magnetic field interaction that a traditional magnetic strip on a conventional credit card can produce when it is passed through a reader. Similar to a traditional plastic credit card, the planar coil can also produce a magnetic field that can be read by a pickup (or "transducer"). The pickup produces electric current in the coil that, in turn, produces a magnetic field that is read by the pickup. Accordingly, the planar coil can be read in the same way as the magnetic strip on a traditional plastic credit card. The magnetic field produced by the planar coil would behave identically to a traditional magnetic strip.

In one embodiment, alongside the main planar coil, auxiliary rate detection assembly independent of the main inductor assembly would be provided to assist with the alignment of the production of data from the loop as it is being passed over the head of the credit card reader. The reader module of a traditional credit card reader comprises a metal head with a small gap on the tip of the head. This gap is where the pickup armature resides, so that when the metal head passes over the credit card strip, an electric field is induced in the head reader pickup circuit. In one embodiment the auxiliary rate detection assembly is constructed of an array of auxiliary inductor coils and magnetic pickup coils, alongside the main coil. As the metal head of the card

reader assembly passes over the arrangement of auxiliary coils and pickup circuits, a disturbance in the magnetic field flowing between the two generates a electrical current change that is detected by a rate detection circuit so as to detect the rate of motion of the card reader head passing across the surface of the card and therefore along the main induction assembly. The purpose of this is to allow the determination of the rate or production of magnetic data symbols in the main inductor assembly to align with the rate at which data is being read by the reader, according to the data density of standard card magnetic strips. Accordingly, it is irrelevant if the credit card of the present invention is being swiped fast or slow, the main inductor assembly produces data at just the right rate depending on the rate at which the card is detected it is being passed over the reader's head.

In one embodiment, a microprocessor is connected to the main coil and the alignment pickups. The microprocessor is responsible for producing the data from the coil at the appropriate rate in accordance with the speed with which the card is swiped through the reader. As shown in FIG. **1**, the auxiliary coil detects the rate at which the credit card is being swiped. The microprocessor then uses this information to produce the data from the main planar coil at the appropriate rate for the credit card reader.

In addition, the credit card of the present invention comprises a real time clock that can produce a cryptographically worthy timestamp for each interaction and a battery back up that can be used to power up the microprocessor. Further, the card can comprise additional human inputs, e.g., touch sensors which can be formed by contacts that a user can press. For example, there can be contacts that a user can press to wake up the card, to cause the battery to supply power, or to put the card to sleep when it is not being used. There can also be additional inputs to key in customer specific information. For example, there can be inputs to key in a password or any other kind of unique identifier. If any other number besides the password is entered multiple times, or if there is attempted usage of the card without entering in a password, an automatic phone call may be triggered to the appropriate fraud protection authorities.

In one embodiment, the number on the front of the card can be a full or partial number. The number may not have to necessarily be a static number. For example, the first four and last four digits of the card number can be fixed while the remaining eight can be dynamically generated. As the credit card is read by the machine, part or all of the number may be dynamically produced at the time the card is read. The dynamic part of the number generated may be based on the user's private information, the user's bank information, the time of day or the facility that is reading the card. Further, the expiration date of the card can also be dynamically generated. Effectively, a credit card can be created that has no fixed number and therefore cannot be stolen. Only the number generated at the instant the card is being used matters. Accordingly, unauthorized use of the card is nearly impossible because no transaction can be conducted with only the partial static part of the payment number. In one embodiment of the present invention, enough dynamically generated numbers are provided for on the credit card such that a unique payment number can be generated for each transaction. In this embodiment, the credit card of the present invention effectively acts as a unique per transaction credit card.

In embodiments of the present invention comprising dynamically created payment numbers, a single credit card can be used for multiple banks. For example, instead of carrying a separate credit card for all the different credit card companies, a customer would only need to carry a single card and one of the inputs on the front of the card can be used to select the appropriate bank or credit provider.

In one embodiment of the present invention, a thin film liquid crystal display ("LCD") can be fitted on the card so the credit card can have a display screen. The display can have multiple uses. In one embodiment, the display can be used to ask the user a security question if an improper password is entered. Or if the fraud protection services need to contact a customer, they can verify the customer's identity by transmitting a security question to the user's credit card screen to which the user would then need to respond correctly using the input buttons on the card.

In one embodiment, the credit card of the present invention could also be used to make online purchases. In this embodiment, the card could use RFID or near field technology so that it can connect to a personal computer and be used to uniquely generate a payment number for online purchases. The number could also, in one embodiment, be displayed on the front LCD of the card. In one embodiment, the card may also be equipped with a means for communicating with the USB port on the computer in connection with making the online purchases.

TABLE 1

1. An apparatus for conducting credit transactions comprising:
a device with the similar dimensions and thickness to a standard credit card
an inductor assembly integrated into said device capable of generating a programmed magnetic field at a location on the device where it will come into proximity to a standard credit card magnetic-strip reader
the inductor assembly being operable to be read by a magnetic pickup of an electronic credit card reader;
at least one auxiliary rate detection units adjacent to said inductor assembly, wherein said at least one auxiliary detection unit is operable to detect a rate at which said device, including said inductor assembly, is passed through said electronic credit card reader; and
a microprocessor operatively coupled to said inductor assembly and said at least one detection unit, wherein said microprocessor is operable to simulate magnetic-strip data fields using the inductor assembly, at a rate determined from said auxiliary detection units.
2. A method of Claim 1, wherein the inductor assembly is a planar coil which is a looped inductor with dimension roughly equal to, and along the axis of, the standard credit-card magnetic strip

TABLE 1-continued

3. A method of Claim 1, wherein said detection assembly consists of a plurality of motion rate detection units, which may comprise inductor coils and companion magnetic-field pickup coils, each of which is able to detect the proximity of metallic objects, such as magnetic-strip reader heads, passing through the magnetic field created by said inductor and detected by said pickup coil.
4. A method of Claim 1, wherein said device may incorporate a plurality of touch sensors arranged along the surface of said device which may; allow user input of information, allow introducing a transaction specific identifier, to confirm/deny transaction information, to operate in sequence, or with a gesture across said sensor for the purpose lock/unlock or control access for transactions
5. A method of Claim 4, wherein said device contains a real-time clock or counter unit which generates a sequential parameter when the card is read by said credit card reader, and which along with certain user information, transaction identifiers, user secrets, payment authority secrets is combined to generate a limited-use payment number, which has a limited recurrence, is limited in scope of use to a predetermined number of authorized transactions
6. A method of Claim 5, wherein the time, sequence, user, payment authority and other information is similarly combined by credit card processing facility to generate a payment number for comparison to the number transmitted by the credit card reader, for the purposes of authenticating said number is from a recognized card used in a user-authorized transaction
7. A method of Claim 1, wherein said device incorporates a display allowing payment number, time, passcodes, sequence codes, amounts and other credit card transaction information to be displayed for user, merchant, bank or credit card authority
8. An Apparatus for conducting credit transactions comprising, wherein the edge of said device contains a connector for connection to standard computing devices such as a USB interface.

The foregoing description, for purpose of explanation, has been described with reference to specific embodiments. However, the illustrative discussions above are not intended to be exhaustive or to limit the invention to the precise forms disclosed. Many modifications and variations are possible in view of the above teachings. The embodiments were chosen and described in order to best explain the principles of the invention and its practical applications, to thereby enable others skilled in the art to best utilize the invention and various embodiments with various modifications as may be suited to the particular use contemplated.

Embodiments according to the invention are thus described. While the present disclosure has been described in particular embodiments, it should be appreciated that the invention should not be construed as limited by such embodiments, but rather construed according to the below claims.

What is claimed is:

1. A method of generating and using limited-use payment information for performing a payment transaction, the method comprising:

receiving an input at an electronic device, wherein the input comprises a priming operation, and, wherein the electronic device comprises:

a processor;

a touch-screen display coupled to the processor; and

a near field communications (NFC) interface coupled to the processor;

responsive to said priming operation, readying said device to perform a payment transaction by an identified user;

receiving a payment request for the payment transaction at said electronic device;

displaying, on the touch-screen display, information reflecting the payment request, and an image representing a selected issued payment account;

dynamically generating, by the processor, limited-use payment information;

wherein said limited-use payment information is dynamically generated based on a per-transaction sequential parameter originating from the electronic device;

using said limited-use payment information in connection with the payment transaction in place of issued payment information associated with said selected issued payment account;

transmitting said limited-use payment information from said electronic device via said NFC interface for receipt by an NFC recipient;

responsive to the transmitting the limited-use payment information, receiving via the NFC interface information reflecting a status of said payment transaction; and

displaying the status of said payment transaction via said touch-screen display.

2. The method of claim **1**, wherein the limited-use payment information comprises a cryptogram number.

3. The method of claim **2**, further comprising:

prior to the priming operation, transmitting the issued payment information for receipt by a payment processing authority; and,

in response to said transmitting issued payment information, receiving a static device account information that is unique to the electronic device.

4. The method of claim **3** further comprising:

combining said limited-use payment information and said static device account information, to reduce a combined payment information;

transmitting said combined payment information, in place of the issued payment account information, via said NFC for receipt by an NFC recipient; and

receiving, via the NFC interface, and in response to transmitting said combined payment information, transaction processing information reflecting a status of said payment transaction.

5. The method of claim **3**, wherein the dynamically generating Lather comprises dynamically generating the limited-use payment information based on payment processing authority secret information.

6. The method of claim 5, wherein the limited-use payment information is based on at least one secret information shared by both the electronic device and the payment processing authority.

7. The method of claim 1, wherein the priming operation comprises bringing the electronic device within receiving proximity of an NFC recipient.

8. The method of claim 7, wherein said readying said device to perform a payment transaction comprises:

identifying said proximity NFC recipient is an NFC payment facility;

successfully validating the identified user as authorized to perform the payment transaction via said electronic device; and

receiving a user approval for performing the payment transaction.

9. The method of claim 8, wherein said user approval for performing a payment transaction comprises displaying a request for user input at said electronic device, for both said identifying and said user approval of said payment transaction, and further comprising:

the processor identifying that said user input matches a known authorized user of the electronic device, before said readying said device to perform a payment transaction; and,

disallowing the payment transaction by the device until said readying said device to perform the payment transaction is successfully completed.

10. The method of claim 8, wherein said successfully validating the identified user comprises the processor successfully determining a match between:

firstly, a user input received via at least one of a set of user input sensors of the electronic device; and,

secondly, at least one of the set consisting of: predetermined user characteristics, and challenge-responses of an authorized user, as stored in the electronic device.

11. The method of claim 10, wherein said user input received via at least one of a set of user input sensors of the electronic device comprises a passcode entry sequence performed by a user input via the touch-screen display.

12. The method of claim 10, wherein said predetermined user characteristics stored within the electronic device comprise known user biometric touch characteristics.

13. The method of claim 10, wherein said predetermined user characteristics stored within the electronic device comprise a known user touch gesture.

14. The method of claim 10, wherein said predetermined user characteristics stored within the electronic device comprise a known user motion of the device.

15. The method of claim 1, wherein the input comprising a priming operation is a user input.

16. The method of claim 15, wherein said readying said device to perform a payment transaction comprises:

successfully identifying said identified user from said user input; and,

wherein said user input further comprises a user approval for performing the payment transaction received from said identified user; and,

wherein said successfully identifying further comprises said electronic device validating an authorized user of said electronic device by comparing a user-touch input received via a touch input sensor on the electronic device with a recognized valid user-touch, stored in a memory of the electronic device; and,

wherein said user approval for performing the payment transaction further comprises:

visually presenting information of the payment transaction on the touch screen display of said electronic device;

visually presenting a request for user approval of the payment transaction via touch input at said electronic device; and,

subsequent to receiving a user-touch input from an identified user, approving performance of said payment transaction via said electronic device.

17. The method of claim 1, further comprising:

prior to the priming operation, transmitting the issued payment information for receipt by a payment processing authority; and,

in response to said transmitting issued payment information, receiving a static device account information that is unique to the electronic device.

18. The method of claim 17 further comprising:

combining said limited-use payment information and said static device account information, to produce a combined payment information;

transmitting said combined payment information, in place of the issued payment account information said NFC interface for receipt by an NFC recipient; and

receiving, via the NFC interface, and in response to transmitting said combined payment information, transaction processing information reflecting a status of said payment transaction.

19. The method of claim 18, wherein the dynamically generating further comprises dynamically generating the limited-use payment information based on payment processing authority secret information.

20. The method of claim 19, wherein the limited-use payment information is based on at least one secret information shared by both the electronic device and the payment processing authority.

21. The method of claim 17, wherein the dynamically generating further comprises dynamically generating the limited-use payment information based on payment processing authority secret information.

22. The method of claim 21, wherein the limited-use payment information is based on at least one secret information shared by both the electronic device and the payment processing authority.

23. The method of claim 1, further comprising:

prior to the priming operation, transmitting the issued payment information, user information and device-specific information; and,

in response to transmitting said issued payment information, user information and device-specific information, receiving a payment processing authority supplied secret information.

24. The method of claim 23 wherein said payment processing authority supplied secret information comprises static device account information.

25. The method of claim 24 wherein said static device account information comprises a static device account number and a static device-specific expiration date.

26. The method of claim 25 wherein the static device account number is associated with the selected issued payment account on said electronic device.

27. The method of claim 1, wherein the dynamically generating further comprises dynamically generating the limited-use payment information based on payment processing authority secret information.

28. The method of claim 27 wherein the limited-use payment information is based on at least one secret information shared by both the electronic device and the payment processing authority; and

further wherein the at least one secret information is not exchanged when preforming the payment transaction.

29. A system for completing a payment transaction, the system comprising:

an electronic device operable to receive a priming operation, wherein the priming operation is operable to ready said device for performing a payment transaction by an identified user, and, wherein the electronic device further comprises:

a processor;

a near field communications (NFC) interface coupled to the processor and operable to receive a payment request associated with the payment transaction; and,

a touch-screen display coupled to the processor, and

wherein the electronic device is operable to cause the display of information reflecting device-readiness, the payment request, and an image representing at least one selected issued payment account;

wherein the electronic device is operable to dynamically generate limited-use payment information based on a sequential counter count from the electronic device;

wherein the electronic device is operable to store a static device-specific user account information;

wherein the electronic device is operable to transmit a combination of said dynamically generated limited-use payment information and said static device-specific user account information to an NFC recipient via, said NFC interface for use in connection with payment transaction in place of information associated with said selected issued payment account;

wherein the electronic device is operable, subsequent to transmission of said combination, to receive a status information reflecting a status of said payment transaction; and,

wherein the touch-screen display is operable to display as indication of said status information.

30. The system of claim 29, wherein the dynamically generated limited-use payment information comprises a cryptogram number.

31. The system of claim 29, wherein the device-specific user account information comprises static device account information.

32. The system of claim 31, wherein the static device account information comprises a static device account number that is unique to the electronic device.

33. The system of claim 32 wherein the static device account information further comprises a static device account expiration date.

34. The system of claim 32 wherein the sequential counter count is changed per payment transaction.

35. The system of claim 34 wherein the electronic device is operable to transmit issued payment account information and in response thereto, to receive the static device account information.

36. The system of claim 29 wherein the electronic device is further operable to dynamically generate the limited-use payment information based on a shared information: from said user, information associated with said electronic device, information associated with said selected, issued payment account, and at least one secret; and,

wherein said shared information is shared by both the electronic device and a payment processing authority.

37. The system of claim 36 wherein the electronic device is further operable to dynamically generate the limited-use payment information based on payment processing authority secrets.

38. The system of claim 29 wherein the electronic device is further operable to dynamically generate the limited-use payment information based on payment processing authority secrets.

39. An electronic device for completing a payment transaction, the electronic device comprising:

a processor;

a memory coupled to the processor, wherein the memory is operable to store information associated with use of an issued payment account and wherein the payment authority information comprises a secret information;

a near field communications (NFC) interface coupled to the processor and operable to receive a payment request associated with the payment transaction;

a user interface coupled to the processor;

a user input device coupled to the processor; and,

wherein said processor is operable to:

responsive to a priming operation, wherein the priming operation is operable to ready the device to perform the payment transaction,

cause the display of information associated with the payment request;

cause the display of an image representing at least one user-selectable issued payment account; and,

dynamically generate a limited-use payment information based on a per-transaction sequential parameter originating from the electronic device, and secret information associated with a selected issued payment account; and,

cause the transmission, via said NFC interface, a payment information combination comprising the dynamically generated limited-use payment information and said payment authority information, for receipt by an NFC recipient;

wherein the NFC interface is operable, in response to transmitting said payment information combination, to receive status information reflecting a transaction processing status of said payment transaction; and

wherein the user interface is operable to provide an indication of the status information.

40. The device of claim 39 wherein the payment authority information comprises information that is unique to the electronic device.

41. The device of claim 39 wherein the payment authority information comprises a secret information shared by both the electronic device and a payment processing authority.

42. The device of claim 41 wherein the processing authority information comprises a static device account number.

43. The device of claim 42 wherein the processing authority information further comprises a static device account expiration date.

44. The device of claim 39 wherein the processor is operable to cause the transmission of issued payment account information and in response thereto, to receive the processing authority information.

45. The device of claim 39 wherein the dynamically generated limited-use payment information comprises a cryptogram number, and further wherein the processor is operable to cause transmission, via said NFC interface, of a payment information combination comprising the dynamically generated limited-use payment information and at least a portion of said payment authority information in connection with the payment transaction in place of at least a

portion of the payment information associated with said selected issued payment account.

46. The device of claim **45** wherein the processor is operable to cause the transmission of issued payment account information and in response thereto, receive the processing authority information.

47. The device of claim **46** wherein the processing authority information comprises a static device account number.

48. The device of claim **47** wherein the processing authority information further comprises a static device account expiration date.

49. The device of claim **39**, wherein said user interface comprises a display and wherein said user input device comprises a touch panel disposed adjacent to said display and wherein further the processor is operable to identify an authorized user by validating a valid user passcode input to the touch panel.

50. The device of claim **39**, wherein said user interface comprises a display and wherein said user input device comprises a touch panel disposed adjacent to said display and wherein further the processor is operable to identify an authorized user by displaying a security challenge question presented on the display and receiving a correct user response thereto.

51. The device of claim **39**, wherein said user input device comprises a biometric sensor operable to detect a user touch of said electronic device and wherein further the processor is operable to identify an authorized user by biometric sensing of a continuous user touch.

52. The device of claim **39**, wherein said user interface comprises a display and wherein said user input device comprises a touch panel disposed adjacent to said display and wherein further the processor is operable to identify an authorized user by biometric sensing of a user touch at the touch panel.

53. The device of claim **39**, wherein said user interface comprises a display and wherein said user input device comprises a touch panel disposed adjacent to said display and wherein further the processor is operable to identify an authorized user by biometric recognition of a valid user identification.

54. The device of claim **39**, wherein said user input device comprises an army of motion sensors and wherein further the processor is operable to identify an authorized user by detecting a recognized user displacement of the array of motion sensors.

55. The device of claim **39**, wherein the processor is operable to:

receive a user-selection of an issued payment account presented on the user interface, received the user input device coupled to the processor, and

responsive thereto, select from the memory a specific processing authority information corresponding to the user-selected issued payment account information, and

use at least a portion of said specific processing authority information in place of at least a portion of the issued payment account information to generate a combined payment information to complete a payment transaction per the input user-selection.

56. An electronic device for completing a payment transaction, the electronic device comprising:

a processor;

a memory coupled to the processor, wherein the memory stores a payment authority information associated with a user-selectable issued payment account, and wherein the payment authority information includes a secret information;

a near field communications (NFC) interface coupled to the processor and operable to receive a payment request associated with the payment transaction;

a user interface coupled to the processor;

a user input device coupled to the processor; and,

wherein said processor is operable to:

responsive to a priming operation, wherein the priming operation is operable to ready the device to perform the payment transaction,

cause the display of information associated with the payment request;

cause the display of an image representing the user-selectable issued payment account; and,

dynamically generate a limited-use payment information based on a per-transaction sequential parameter originating from the electronic device, and the secret information associated with the user-selectable issued payment account; and,

cause the transmission, via said NFC interface, of a payment information combination comprising, the dynamically generated limited-use payment information and at least a portion of said payment authority information, for receipt by an NFC recipient;

wherein the NFC interface is operable, in response to transmitting said payment information combination, to receive status information reflecting a transaction processing status of said payment transaction; and

wherein the user interface is operable to provide an indication of the transaction status information.

57. The device of claim **56**, wherein the payment authority information comprises information that is unique to the electronic device.

58. The device of claim **57**, wherein the payment authority information comprises a static device account number.

59. The device of claim **58**, wherein the payment authority information further comprises a static device account expiration date.

60. The device of claim **56**, wherein the secret information is shared by both the electronic device and a payment processing authority.

61. The device of claim **56**, wherein the processor is operable to cause the transmission of issued payment account information and in response thereto, to receive the payment authority information.

62. The device of claim **56**, wherein the dynamically generated limited-use payment information comprises a cryptogram number, and further payment information combination is used in place of at least a portion of fixed payment information associated with said user-selectable issued payment account.

63. The device of claim **62**, wherein the processor is operable to cause the transmission of issued payment account information and in response thereto, receive the payment authority information.

64. The device of claim **63**, wherein the payment authority information comprises a static device account number.

65. The device of claim **64**, wherein the payment authority information further comprises a static device account expiration date.

66. The device of claim **56**, wherein said user interface comprises a display and wherein said user input device comprises a touch screen interface of the display, and wherein further the processor is operable to identify an authorized user by validating a valid user passcode input to the touch screen interface.

67. The device of claim **56**, wherein said user interface comprises a display and wherein said user input device

comprises a touch screen interface of the display, and wherein further the processor is operable to identify an authorized user by displaying a security challenge question presented on the display and receiving a correct user response via said touch screen interface of the display.

68. The device of claim **56**, wherein said user input device comprises a biometric sensor operable to detect a user touch of said electronic device and wherein further the processor is operable to identify an authorized user by biometric sensing of said user touch.

69. The device of claim **56**, wherein said user interface comprises a display and wherein said user input device comprises a touch screen interface of the display and wherein further the processor is operable to identify an authorized user by biometric sensing of a user touch at the touch screen interface.

70. The device of claim **56**, wherein said user interface comprises a display and wherein said user input device comprises a touch input of the electronic device and wherein further the processor is operable to identify an authorized user by biometric recognition of a valid user identification via the touch input.

71. The device of claim **56**, wherein said user input device comprises an array of motion sensors and wherein further the processor is operable to identify an authorized user by detecting a recognized user displacement of the array of motion sensors.

72. The device of claim **56**, wherein the processor is operable to receive, via the user input device, a user-selection of said user-selectable issued payment account presented on the user interface, and

in response thereto, is further operable to select from memory the payment authority information corresponding to selected user-selectable issued payment account, and

is further operable to use said payment information combination in place of at least a portion of fixed payment information associated with said selected user-selectable issued payment account.

* * * * *